

3 1761 11648464 3

CA1
PC
- A57

142

Government
Publications

Privacy Commissioner
of Canada




Commissaire à la protection
de la vie privée du Canada

142

Privacy

ANNUAL REPORT

TO PARLIAMENT 2002-2003



Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

<https://archive.org/details/31761116484643>

142

Privacy Commissioner
of Canada

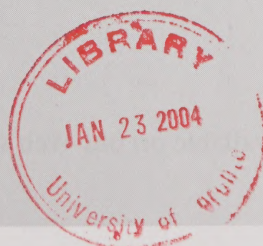


Commissaire à la protection
de la vie privée du Canada

Privacy

ANNUAL REPORT

TO PARLIAMENT 2002-2003



Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376

Fax (613) 947-6850

TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2003

Cat. No. IP30-1/2003

ISBN 0-662-67544-4

This publication is also available on our Web site at www.privcom.gc.ca

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télééc.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



September 2003

The Honourable Daniel Hays, Senator
The Speaker
The Senate of Canada
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report for the Office of the Privacy Commissioner of Canada, for the period from April 1, 2002 to March 31, 2003 for the *Privacy Act* and from January 1 to December 31, 2002 for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

A handwritten signature in black ink, reading "Robert Marleau".

Robert Marleau
Interim Privacy Commissioner
of Canada

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télééc.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



September 2003

The Honourable Peter Milliken, M.P.
The Speaker
The House of Commons
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report for the Office of the Privacy Commissioner of Canada, for the period from April 1, 2002 to March 31, 2003 for the *Privacy Act* and from January 1 to December 31, 2002 for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

A handwritten signature in cursive script, reading "Robert Marleau".

Robert Marleau
Interim Privacy Commissioner
of Canada

Table of Contents

Foreword.....	1
Overview	3
Substantially Similar Provincial Legislation	13
Part One - Report on the <i>Privacy Act</i>	17
Introduction.....	17
Investigations and Inquiries	18
Complaints under the <i>Privacy Act</i>	19
Definitions of findings under the <i>Privacy Act</i>	21
Summary of select cases under the <i>Privacy Act</i>	22
Incidents under the <i>Privacy Act</i>	35
Public Interest Disclosures	37
Privacy Practices and Reviews.....	45
Privacy Impact Assessments.....	47
In the Courts.....	51
Part Two - Report on the <i>Personal Information Protection and Electronic Documents Act</i>	55
Introduction.....	55
Investigations and Inquiries	56
Definitions of findings under the <i>PIPED Act</i>	57
Summary of select cases under the <i>PIPED Act</i>	58
Incidents under the <i>PIPED Act</i>	88
Privacy Practices and Reviews.....	91
In the Courts.....	92
Part Three - Corporate Services	97

Foreword

My presenting this Annual Report for the fiscal year 2002-2003 may seem something of an oddity. I was appointed interim Privacy Commissioner in July of this year, well past the end of the reporting period, so I cannot take credit for any of the work that is reported here. But in fact this is less a real problem than it might seem. There is a lot more to the Office of the Privacy Commissioner than just the Commissioner, and even if I had been here for the entire time, it would be a fiction to call this “my” Annual Report. It reflects the work of very talented and dedicated individuals.



These are challenging times for the Office. For one thing, the task of protecting privacy has never been more arduous, what with new private sector legislation, a wide array of proposed anti-terrorist and security measures, and the increasing availability and sophistication of privacy-invasive technologies.

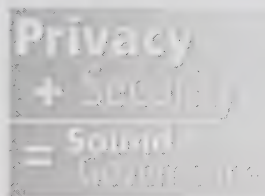
To complicate matters, the Office has undergone a period of intense public scrutiny and organizational disruption. The House of Commons Committee on Government Operations and Estimates conducted an inquiry into operational and administrative issues in the Office, and uncovered a number of

serious problems. As important and necessary as this exercise of Parliamentary oversight is, there is no denying that it, along with the accompanying media attention, has made it difficult for staff of the Office to conduct their work effectively.

I accepted the position of Privacy Commissioner on an interim basis in order to lead the Office through the process of rebuilding itself and repairing its relationship with Parliament and Canadians. Our task now is to regain the confidence of Parliament and our stakeholders, demonstrate to Canadians that they will receive top-level service in protection of their privacy rights, and ensure that organizations understand their obligations, and citizens their rights, when the *Personal Information Protection and Electronic Documents Act* comes fully into effect on January 1, 2004.

I have been impressed by the commitment of the Office's staff, and look forward to working with them in this exciting time. I am confident that from this period of renewal will emerge a new enthusiasm for the cause of privacy and a centre of excellence for its protection and promotion.

Overview



It is common to introduce an Annual Report with some remark about it providing an opportunity to reflect. In the case of this Report, that is not simply a throwaway introduction. The period under review has been an important one for privacy.

For one thing, privacy in our society has been in some danger. This of course is nothing new; privacy has never been something that we can take for granted, and particularly since the advent of computerization it has required active effort to preserve it. But if the danger to privacy is not new, it is intensified. The forces that have ground away at privacy for the last decade—technological advances in the collection, processing, matching, and analysis of personal information, growing pressure to identify and authenticate parties to electronic transactions, and the drive for security from crime and terrorism—have been particularly powerful in the last year.

Public security measures against crime and terrorism have certainly been the most acute and obvious challenge. They also present the most obvious challenge to privacy advocates and Privacy Commissioners, who must walk a fine line between protecting privacy and making life easier for criminals and terrorists.

But in fact the other forces threatening privacy are no less challenging, and arguing for privacy in the face of them often requires walking similar fine lines. Data matching catches people defrauding the system. Identity cards can make it harder for someone to fraudulently use your credit card. Electronic health records can facilitate diagnosis and treatment, and prevent costly or deadly medical mistakes. Giving researchers access to our personal health information can enable research that can prolong life and reduce suffering.

No one would argue with the goals of these measures. But privacy is not simply a frill or a selfish extravagance that can be tossed away the moment someone claims that it inhibits some other valuable social goal—regardless of whether the goal is security or public health or even individual life or death. Privacy is a cornerstone of individual freedom. It exists in a dynamic balance with our other social needs. The key to preserving privacy is careful analysis of any measure that purports to bring us some other social benefit, to ensure that the balance is maintained.

The results of our work in the past year have been mixed. We have continued to manage a large caseload of complaints and ensure that Canadians enjoy full protection of their rights under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. On more general questions of promoting and protecting privacy, we have made some important advances. We have also had some setbacks, and, on a couple of fronts, we have been forced to rethink our approach.

The Office achieved a successful outcome when it spoke up about the Canada Customs and Revenue Agency's proposed database about airline passengers.

This database, as initially proposed, was to contain extensive information on the foreign travel activities of Canadians—where

*On more general
questions of promoting
and protecting privacy,
we have made some
important advances.*

and with whom they travel, how they paid for their tickets, their contact addresses and telephone numbers, even their dietary and health-related requirements. The information would have been retained for seven years, and would have been available for a wide range of administrative and law enforcement purposes.

The impact of this would have been enormous, and unprecedented. The ordinary travel activities of law-abiding people, activities that previously would have passed unnoticed unless there were some reasonable grounds to suspect them, would have been recorded and retained, attached to their names. It would be one more loss of anonymity and privacy, one more way in which innocent people would be identified, tagged, and monitored by the state—in short, one more infringement of the right to privacy.

Our staff analyzed this proposal and concluded that the supposed security benefits to be gained did not justify the infringement of privacy that it represented. Our opposition, supported by public opinion, eventually led the Minister of National Revenue to revise the initiative, significantly reducing the impact on privacy.

One successful outcome does not make a great year. We continue to have concerns about other security initiatives, such as the provisions of the proposed *Public Safety Act* allowing the police to scan all airline passengers against outstanding arrest warrants, the “Lawful Access” proposals to enhance state powers to monitor electronic communications, the proposal for a national identification card, and the growth of police video surveillance of public streets.

One long-running dispute, about the confidentiality of census returns, appears headed for resolution in a manner that runs directly counter to the recommendations of our Office.

Canadians have been told at least since 1905 that the information they reveal in censuses will be held in confidence and only used for statistical purposes. The *Privacy Act* actually allows the National Archives to disclose personal

information collected in a census, 92 years after the information was collected. This remained largely academic until recently, because the only census records under the control of the Archives were those few that had been conducted up until 1901. Census officials took the view that, beginning with the 1906 census, regulations and legislation required them to keep the returns confidential rather than transfer them to the Archives.

Historians and other researchers have long sought access to these documents, and this year the government, following the recommendations of an expert panel but over our objections, released the 1906 census records and introduced legislation to allow the release of the rest.

Our Office had supported a compromise that would have limited access to the returns to scholars conducting peer-reviewed historical research and individuals wishing to conduct genealogical research on their own families. The government rejected this.

Our concern is with the repeated promises of confidentiality. Canadians were asked to reveal personal information to census-takers, and were led to believe that it would be kept confidential. Violating that promise could diminish the confidence Canadians have in government. We remain hopeful that this will be recognized when the House of Commons takes up this proposed legislation, which was passed by the Senate in May.

On another important privacy issue, video surveillance of public streets, we concluded that a new approach needs to be taken. The previous Commissioner had initiated a lawsuit in the British Columbia Supreme Court, alleging that the RCMP's video surveillance of a public street in Kelowna, B.C., violated the *Canadian Charter of Rights and Freedoms*. The Court, however, did not address the substance of the case at all. It ruled that the Privacy Commissioner simply does not have the capacity to launch such an action, and dismissed it on that basis.

This presented us with something of a quandary. On the one hand, video surveillance of public places has serious privacy implications, so the idea of simply

letting the issue drop because of a procedural problem seemed hardly satisfactory. On the other hand, regardless of what we wanted, the issue had become the one defined by the Court. If we had appealed the decision, the appeal would have been about that issue alone. To work our way through two more levels of appeal would have taken years, at the end of which we would have spent a great deal

of the Office's energies and a considerable amount of public money, without any answer from a court on the substantive issue of video surveillance. The issue has to be addressed, but it must be done in a different way. Accordingly, we withdrew the case, but we will pursue this issue with determination.

*It was striking this
past year how many
of our privacy concerns
are tied up with
anonymity and its
opposite pole, identity.*

It was striking this past year how many of our privacy concerns are tied up with anonymity and its opposite pole, identity. The ability to conduct the majority of our daily activities in an anonymous fashion is one of the keys to our keeping control of information about us. People can have a private life even if much of their lives is spent in public view, as long as their activities cannot be linked to each other and to themselves. It is the ability to connect activities to each other and to an identifiable person that is at the heart of profiling and surveillance.

This perspective ties together our concerns about such superficially different things as authentication of clients in electronic transactions, biometric facial recognition systems in airports, traveller databases, and a national identification card.

This was the view that we tried to impress upon the House of Commons Standing Committee on Citizenship and Immigration in its hearings on whether Canada needs a national identification card. We made the argument that such a card (whatever the details of the proposal are, and to date there is

no real proposal) would do little to address real problems, would present enormous financial and practical challenges to implement, and would do grave damage to privacy.

While the Office has wide-ranging interests and strives to serve as Parliament's window on all privacy issues, the heart and soul of its work is the system of enforceable privacy rights set up under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*.

On this account, 2003 was a noteworthy year. First of all, it marks the 20th anniversary of the *Privacy Act*. That calls for reflection not just on the past year, but on the past twenty, and in particular on the model of privacy protection that Parliament adopted with the *Privacy Act*. That model is based around an Officer of Parliament, the Privacy Commissioner, who advises Parliament on privacy issues, analyzes the implications of legislative and regulatory initiatives so that Parliamentarians and Canadians can make informed decisions, and acts as an ombudsman to protect privacy rights, through negotiation, persuasion and dialogue—and occasionally, as a last resort, through publicity. The system set up under the *Privacy Act* quickly showed itself to be a useful one, and it was no surprise that it was adopted and applied to the private sector when Parliament passed the *Personal Information Protection and Electronic Documents Act*.

We are confident that in the past year, this system has proved useful to Parliament, and indeed has been reaffirmed. Parliament has rethought and revised legislative initiatives such as the CCRA database so as to minimize impacts on privacy, and we think that the outlook for privacy in Canada, despite all the pressures, is encouraging.

The year 2003 is important for the other statute we administer, the *Personal Information Protection and Electronic Documents Act* or PIPED Act as we call it, since this is the last year before it reaches its full application. The Act has been coming into force in stages. At the outset, in 2001, it applied to certain commercial exchanges of information but excluded personal health information. As of January 2002, it extended to include personal health information. The

final stage will begin in January, 2004, when the Act will apply to all commercial activity in Canada except where provinces have passed substantially similar legislation. (To date, only Quebec has privacy legislation deemed substantially similar, but both British Columbia and Alberta introduced legislation this year, another promising sign for privacy protection in Canada.)

In general, the introduction and implementation of the Act have gone far more smoothly than some had predicted. The business community has responded well to the demands of complying with the legislation, and while there have been some bumps in the road, on the whole the new way of doing business has not been as difficult or traumatic as some had predicted. We are seeing a general recognition that respecting privacy is not as onerous as some people thought, and in fact is simply good business practice. One of the most encouraging signs is the obvious interest in compliance among the business community. In fact, a sort of compliance cottage-industry has sprung up, with a host of consulting firms offering expertise in compliance with the Act. Hardly a week goes by without our receiving a brochure for a seminar or workshop about the *PIPED Act*.

And the ombudsman model, which proved itself under the *Privacy Act*, has also worked well with respect to the *PIPED Act*. We have been encouraged by the willingness of private sector organizations subject to the Act to comply with the requirements in the legislation and to recognize the Office's specific expertise in getting to the bottom of privacy issues.

As far as day-to-day operations are concerned, the Office continued to face significant challenges, but it remains a resilient and healthy organization in the face of heavy public demand for its services. We

*We are seeing a general
recognition that
respecting privacy is not
as onerous as some
people thought, and in
fact is simply good
business practice.*

dealt with a heavy caseload of complaints under the *Privacy Act*, including a 35% increase in new complaints over last year. Under the *PIPED Act*, the number of new complaints almost tripled over last year, and we can expect a significant increase with the extension of the application of the Act in 2004.

An important development in the past year was the introduction of the Treasury Board's new policy on privacy impact assessments.

A privacy impact assessment, or PIA, is quite simply an assessment of how, and how much, a program or activity affects the privacy of individuals. Typically, it will entail a description of the program, an analysis of what will happen to the personal information collected, used, and disclosed, and an assessment of the program's compliance with privacy principles, legislation, and policies. The Treasury Board's new policy makes PIAs a condition of funding for all new, substantially redesigned, or electronically driven programs and services that collect, use, or disclose personal information. Canada is the first country in the world to make PIAs mandatory in this way.

The implementation of this policy means that government institutions will have to look at privacy right from the outset, from the moment they begin planning a new program. The significance of this is that questions of whether a program or project has a negative effect on privacy—whether it will entail new data matching or increased sharing of personal information, for example, or result in the development of new common personal identifiers, or extended use of existing ones—will be asked before any privacy violation occurs. This preventive approach, rather than a punitive or remedial one, is the most sensible approach to an issue like privacy. Once privacy is violated, once an individual's personal information has been taken out of his or her control, it cannot be undone. Lost privacy cannot be given back. That is why Treasury Board's policy is so

*So it has been a year of
some good news, some
disappointments, and
many continuing
challenges.*

welcome. When government initiatives add to sound governance, it should be recognized and applauded.

So it has been a year of some good news, some disappointments, and many continuing challenges. Fortunately, we have not had to face all our challenges alone. The protection of privacy involves us in a continuing dialogue, in Canada and abroad, with privacy advocates, civil libertarians, academics, and, of course, other privacy and data protection commissioners. They have helped us to bear the burden of the disappointments, and they deserve full credit for their part in bringing about the good news.

The Standing Committee on Government Operations has done its duty in holding this Office accountable to higher standards of prudence and probity in the use of public funds. As we move forward in another watershed year for privacy issues, the Office of the Privacy Commissioner will work for renewed support from the Senate and the House of Commons to blunt the impact of pervasive and invasive technologies and policies on the privacy rights of Canadians.

Substantially Similar Provincial Legislation

Under paragraph 26(2)(b) of the *Personal Information Protection and Electronic Documents Act*, the Governor in Council can exempt an organization, a class of organizations, an activity or a class of activities from the application of *PIPED Act* with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation deemed to be substantially similar to the *PIPED Act*.

The intent of this provision is to allow provinces and territories to regulate the personal information management practices of organizations operating within their borders, provided that they have in place a law that is substantially similar.

If the Governor in Council issues an Order declaring a provincial act to be substantially similar, the collection, use or disclosure of personal information by organizations subject to the provincial act will not be covered by the *PIPED Act*. Personal information that flows across provincial or national borders will be subject to the *PIPED Act* and the *PIPED Act* will continue to apply within a province to the activities of federal works, undertakings and businesses that are under federal jurisdiction such as banking, broadcasting, telecommunications and transportation.

On September 22, 2001, Industry Canada published a notice in the *Canada Gazette* Part 1 setting out the process that the department will follow for determining whether provincial/territorial legislation will be deemed substantially similar.

The process will be triggered by a province, territory or organization advising the Minister of Industry of legislation that they believe is substantially similar to the *PIPED Act*. The Minister may also act on his or her own initiative and recommend to the Governor in Council that provincial or territorial legislation be designated as substantially similar.

The Minister has stated that he will seek the Privacy Commissioner's views on whether or not legislation is substantially similar and include the Commissioner's views in the submission to the Governor in Council.

The process also provides for an opportunity for the public and interested parties to comment on the legislation in question.

According to the *Canada Gazette* notice, the Minister will expect substantially similar provincial or territorial legislation to:

- incorporate the ten principles in Schedule 1 of the *PIPED Act*;
- provide for an independent and effective oversight and redress mechanism with powers to investigate; and
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

In addition to providing comments to the Minister of Industry with respect to specific provincial or territorial legislation, the

The process also provides for an opportunity for the public and interested parties to comment on the legislation in question.

Privacy Commissioner is required by subsection 25(1) to report annually to the Parliament of Canada on the “extent to which the provinces have enacted legislation that is substantially similar to the *PIPED Act*.”

The previous Commissioner issued two reports to Parliament on the matter of substantially similar provincial legislation. In May 2002, he issued a report in which he concluded that Quebec’s *An Act Respecting the Protection of Personal Information in the Private Sector* is substantially similar to the *PIPED Act* in terms of the extent to which it protects personal information. In June 2003, the previous Commissioner issued a second report in which he raised concerns about Bills 44 and 38 that have been introduced, but not yet passed, by the provinces of Alberta and British Columbia, respectively.

As neither Bill has been passed, we will continue to monitor their progress and maintain a dialogue with our provincial counterparts.

Part One

Report on the *Privacy Act*

INTRODUCTION

The *Privacy Act*, which has been in force since 1983, protects individuals' privacy with respect to personal information held by federal Government institutions. The *Act* governs how federal institutions collect, use, disclose and dispose of personal information, and it gives individuals rights to request access to and correction of their personal information. It also sets out the Privacy Commissioner of Canada's duties, responsibilities and mandate.

The Privacy Commissioner receives and investigates complaints from individuals who believe their rights under the *Act* have been violated. The Commissioner can also initiate a complaint and investigation himself, in any situation where there are reasonable grounds to believe the *Act* has been violated.

As an ombudsman, the Commissioner's first priority is to resolve complaints to the extent possible, through mediation and negotiation if that becomes necessary. But the *Act* also gives the Commissioner broad investigative powers – he can subpoena witnesses and compel testimony, enter premises to obtain documents and conduct interviews. Obstructing an investigation is an offence under the *Act*. While the *Act* does not grant the Commissioner any order-making powers, the Commissioner can recommend changes to the way

Government institutions handle personal information, based on findings in a complaint.

The Commissioner also has a mandate to conduct periodic audits of federal institutions and to recommend changes to any practices that he considers not being in compliance with the *Privacy Act*.

The *Act* requires the Commissioner to submit an Annual Report to Parliament on the activities of his Office in the previous fiscal year. The current Report covers the period from April 1, 2002 to March 31, 2003 for the *Privacy Act*.

INVESTIGATIONS AND INQUIRIES

The Office's Investigations and Inquiries Branch is responsible for investigating complaints received from individuals under section 29 of the *Privacy Act* (and section 11 of the *Personal Information Protection and Electronic Documents (PIPED) Act*, which is discussed later in this Report).

Essentially, these investigations serve to establish whether individuals have had their privacy rights violated and whether they have been accorded their right of access to their personal information.

Where privacy or access rights have been violated, the investigation process seeks to provide redress for individuals and prevent violations from reoccurring.

The *Privacy Act* gives the Commissioner the authority to administer oaths, receive evidence and enter premises where appropriate, and examine or obtain copies of records found in any premises.

We are pleased to note that we have had voluntary co-operation to date, and all complaints brought before the Commissioner and his predecessors have been resolved without having to use these formal investigative powers.

The Investigations and Inquiries Branch also responds to thousands of inquiries annually from individuals and organizations contacting the Office for advice and assistance on a wide range of privacy-related matters.

Complaint Investigations Closed

April 1, 2002 to March 31, 2003

2001-2002:	1,673
2002-2003:	3,483

COMPLAINTS UNDER THE *PRIVACY ACT*

During the current reporting year, this Office received 1,642 new complaints. Approximately 43% were filed by individuals alleging that their access rights under the *Privacy Act* had been violated; 24% concerned allegations that the confidentiality provisions of the *Act* with regard to collection, use, disclosure, retention and disposal of personal information had not been respected; and the remaining 33% were about the tardiness of Government institutions in responding to requests for access to personal information.

More than two-thirds of the total received were lodged against five federal Government institutions – Correctional Service of Canada, the Canada Customs and Revenue Agency, the Royal Canadian Mounted Police, the Department of National Defence, and Citizenship and Immigration Canada.

The former Commissioner issued findings on 3,483 complaints during the year. It is important to note that this figure includes 2,323 complaints related to the Canada Customs and Revenue Agency's (CCRA) disclosure of personal information on Customs' E-311 declaration cards to Human Resources Development Canada (HRDC).

At issue was whether there was sufficient authority to justify the use of personal information collected by the CCRA for one purpose – to declare goods

a traveller is bringing into Canada – for use by HRDC for a totally unrelated purpose – in an investigative data match program to identify returning travellers who were fraudulently receiving employment insurance benefits while outside the country.

The matter had been referred to the Court for an opinion on whether the disclosure was authorized by section 8(2)(b) of the *Privacy Act* and section 108 of the *Customs Act* and whether the use of that information by HRDC as evidence against the individuals contravened their rights under the *Canadian Charter of Rights and Freedoms*.

The Supreme Court of Canada ruled that the disclosure was permissible based on its interpretation of these provisions of the *Privacy Act* and the *Customs Act*. The Court also upheld the lower Court's decision that, based on the limited nature of the information disclosed, there was no reasonable expectation of privacy and as a consequence travellers had not been denied their right under the *Charter* to be secure from unreasonable search or seizure. On that basis, the former Commissioner was required to report to the complainants that their complaints were not well-founded.

Of the remaining 1,160 completed cases, 486 dealt with access matters, 293 dealt with collection, use, disclosure, retention and disposal of personal information, and 381 dealt with time limits. The 3,483 complaints were concluded as follows:

Not well-founded	2,711
Well-founded	371
Well-founded/resolved	77
Resolved	13
Settled	235
Discontinued	76

DEFINITIONS OF FINDINGS UNDER THE *PRIVACY ACT*

Not Well-founded: A finding that a complaint is *not well-founded* means that the investigation uncovered no evidence to lead the Commissioner to conclude that the Government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: A finding that a complaint is *well-founded* means that the Government institution failed to respect the *Privacy Act* rights of an individual. This would also be the Commissioner's finding in a situation where the Government institution refuses to grant access to personal information, despite our recommendation that it be released. In such a case, the next step could be to seek a review by the Federal Court of Canada.

Well-founded/Resolved: The Commissioner will find a complaint to be *well-founded/resolved* when the allegations are substantiated by the investigation and the Government institution has agreed to take corrective measures to rectify the problem.

Resolved: *Resolved* is a formal finding that reflects the Commissioner's role as an ombudsman. It's for those complaints where *well-founded* would be too harsh to fit what essentially is a miscommunication or misunderstanding. It means that this Office, after a full and thorough investigation, has helped negotiate a solution that satisfies all the parties.

Settled during the Course of the Investigation: This is not a formal finding but an acceptable means to dispose of a complaint when the investigation is completed, and the complainant is satisfied with the efforts of this Office and doesn't wish to pursue the issue any further. The complainant retains the right to request a formal finding. When that happens, the investigator re-opens the file, and submits a formal report, and the Commissioner reports the findings in a letter to the complainant.

Discontinued: This means that the investigation was terminated before all the allegations were fully investigated. A case may be *discontinued* for any

number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion. The Commissioner does not issue a formal finding in discontinued complaints.

SUMMARY OF SELECT CASES UNDER THE *PRIVACY ACT*

CIC was collecting income tax information from Canadian employers

Three individuals who wished to employ live-in caregivers from the Philippines complained to this Office that the Canadian Embassy in Manila was asking them to provide sensitive income tax information before it would issue visas to their prospective caregivers. The individuals were worried about sending tax documents containing their social insurance numbers (SINs) and detailed information about their financial situation to a foreign country, especially with identity fraud having become such a major concern.

Citizenship and Immigration Canada (CIC) explained that the Live-In Caregiver Program (LCP) brings qualified caregivers to Canada in situations where there are no Canadians or permanent residents available to fill certain positions. Canadians wishing to hire a caregiver from abroad are required to have their job offer validated through Human Resources Development Canada (HRDC) and to sign a form declaring that they can financially support the person they will employ.

After the job offer was validated by HRDC, the Visa Section of the Canadian Embassy in Manila asked the prospective employers to send their Notice of Assessment for the last two years, their T-4 slips and a letter from their employer confirming employment.

CIC claimed that the information was necessary to determine the *bona fides* of an employment offer and to confirm that the employers were financially capable of supporting a caregiver.

When questioned about its authority to collect income tax information for the purpose of issuing visas to third parties, CIC referred to section 203 of the *Immigration and Refugee Protection Regulations*. A review of that document indicated that the visa officer must determine if the job offer is genuine and if the employment of the foreign national is likely to have a neutral or positive economic effect on the labour market in Canada.

In the previous Annual Report, the former Commissioner stated his position concerning the collection of income tax information without legislative authority. He explained that he found it untenable that an income tax return can be demanded from an individual for a purpose other than that required by law. Canadians should never be required to compromise a fundamental right in order to do business with the Government.

This Office presented those arguments to CIC and, as a result, the Embassy in Manila confirmed that it has ceased asking for income tax information for the purpose of issuing visas to live-in caregivers.

CCRA collected medical information for tax purposes

We received a complaint from a family who alleged that the Canada Customs and Revenue Agency (CCRA) had improperly collected their personal information from a provincial medical insurance plan. The family moved to Africa for three years and before leaving Canada the husband consulted with the CCRA and was told that, for tax purposes, he would be considered a non-resident during his absence from the country. Yet upon returning to Canada he was told that he did not meet the requirements for non-resident status and was taxed accordingly. He later obtained his personal information following a *Privacy Act* request to the CCRA and learned that it had asked the provincial insurance provider for all medical records about him, his wife and his children—including records originating some eight months prior to their departure for Africa and almost 2 1/2 years after their return to Canada.

We established that in order to qualify for non-resident status for tax purposes the CCRA must be satisfied that an individual has sufficiently severed ties

with Canada after moving to another country. The CCRA relies on provisions of the *Income Tax Act* as its authority to obtain sufficient information in order to assess non-residency status. It routinely conducts inquiries when assessing an individual's status, including verifying whether the individual continues to make claims under a provincial medical insurance plan during the time absent from Canada. The fact that an individual made such a claim could be an indication that all ties with Canada had not been severed.

The former Commissioner was satisfied that the CCRA had the necessary authority under the *Income Tax Act* to collect personal information about each family member from the province in order to make a determination on their residency status. Nevertheless, he was concerned about the *extent* of the medical information collected, particularly the information for the periods of time both before the family left the country, and after it returned. CCRA officials did not disagree with the concern that requesting medical information for the 2 1/2-year period after the family's return was excessive.

Under the circumstances, the former Commissioner determined that the CCRA collected more personal information than was necessary and, as a result, had exceeded its authority under section 4 of the *Privacy Act*. He found the complaints well-founded and recommended that the CCRA destroy the information that it obtained from the province.

Inadvertent disclosure of sensitive medical information by ATIP

Personal health information – information about the state of our bodies and minds – is arguably the most private information of all. When that information is not treated with the utmost care and confidentiality, the consequences can be disastrous. A case in point: an individual submitted an *Access to Information Act* (ATIA) request to a Government institution for all documents concerning the appointment of another Government employee to a specific position. The names of the two individuals were only vaguely similar. Yet because the departmental Access to Information and Privacy (ATIP) office's analyst had not taken care to properly read the individuals'

names when processing the ATIA request, an assumption was made that the requester and the appointee were one and the same individual. Thus, virtually all the information in the staffing file was disclosed to the ATIA requester – a small amount of third party information was removed. The file contained information about the appointee that was extremely private in nature – extensive medical

and financial information, information about his family, his own employment and education history, and his home address and telephone number. It was also discovered that there was an uncomfortable history between the two individuals and that the requester had subsequently used some of the appointee's medical information to conduct his own personal inquiries about the appointee.

Following an investigation the institution readily admitted the error, apologized to the individual for what had occurred and gave him a copy of the same package the requester received so that he could see exactly what information about him had been improperly disclosed. The institution also asked the requester to return the information and to not keep any copies of it. While he returned the information, there were no assurances that copies had not been kept. Even had assurances been given, the damage had already been done and the appointee's personal information had already been further disclosed by the requester.

The former Commissioner accepted the fact that the situation occurred as a result of careless human error, but was appalled that the mistake was made at all – especially by the very people within the institution who are supposed to be the resident experts on the protection of personal information. Had the appointee's personal information been reviewed with the care it deserved this grievous violation of his privacy rights would never have occurred.

*When that information
is not treated with the
utmost care and
confidentiality, the
consequences can
be disastrous.*

Disclosure of criminal past to offender's family members

An individual complained to this Office that a Correctional Service Canada (CSC) employee disclosed information about his criminal past to members of his family (including his young children who were previously unaware of their father's past) and to the public. A number of years ago the individual had been incarcerated in the same federal institution where the officer worked and he alleged that the officer disclosed confidential information obtained in the course of his duties.

The individual had also filed a complaint with CSC, which in turn conducted its own investigation. From the outset, the complainant never wavered in his statements that the officer disclosed his personal information. The officer maintained that it was not he who made the remarks, but rather a friend who was present at the time the disclosure took place – an individual he refused to identify either to us or to CSC. All of our efforts to locate the friend met with negative results. Still, based on all of the information we gathered during our investigation, the former Commissioner was prepared to find that the rights afforded the complainant under the *Privacy Act* had been violated as a direct result of the officer's actions. Indeed, CSC concluded that the officer had contravened its Code of Discipline and that he failed to observe the provisions of the *Privacy Act*; he was subsequently suspended for 15 days without pay.

Before rendering his final decision in the matter, the former Commissioner questioned CSC's rationale for concluding that a three-week suspension was appropriate to the circumstances. It was only then that we learned that new developments in the case had caused CSC to reverse its decision and withdraw the officer's suspension. Given the disciplinary action meted out to the officer, his friend had come forward saying that it was he who had disclosed the complainant's personal information, not the officer. While not fully convinced of the friend's credibility – and despite apprehensions in that regard – CSC nevertheless withdrew the suspension.

In light of this new information we conducted further inquiries but found no reason to believe the friend's version of events. Based on the evidence we

obtained, the former Commissioner concluded that it was the officer who disclosed the individual's personal information and that his friend likely only came forward because the repercussions to the officer turned out to be greater than anticipated. The former Commissioner therefore found the complaint well-founded and asked that CSC reconsider the reversal of its decision.

The former Commissioner also advised CSC that it should have advised our officials that the officer's friend had finally come forward after all of the attempts of both CSC and this Office had failed to find him. The former Commissioner considered this to be an extremely important development, one which caused CSC to reverse its initial decision and one which could obviously have had a direct bearing on his decision. CSC was well aware that we had an active investigation into the allegations made by the complainant and, in the former Commissioner's view, CSC should have immediately alerted our officials to the change of events. The former Commissioner received assurances that this was an isolated incident which would not reoccur.

Even a public record should be protected

An individual received an envelope, by courier and addressed to him, containing the Canada Pension Plan (CPP) appeal documents of another individual. He believed that the other individual must have received his own appeal information in error.

Our investigation into this matter confirmed these fears. The other individual had indeed received the complainant's appeal information from HRDC. The mix-up was the result of a lack of attention when the documents were inserted in the envelopes to be sent out.

Section 8 of the *Privacy Act* limits how Government institutions may disclose personal information. In essence, institutions may not disclose personal information to third parties without the consent of the person to whom the information relates, unless one of the permitted disclosures set out in section 8(2) of the *Act* applies.

HRDC explained that the information about the complainant that was disclosed consisted of documents that had been filed at the Federal Court and thus were part of a public record. Since section 69(2) of the *Privacy Act* states that section 8 does not apply to personal information that is publicly available, HRDC contended that it had not contravened the *Act* by sending out the information to the wrong individuals by mistake.

The former Commissioner disagreed because the complainant's information was not disclosed from a public record. The fact that it could be found in a public record does not negate the fact that HRDC disclosed the complainant's information to someone who had no need to know. On that basis, the former Commissioner concluded that the complaint was well-founded.

As a result of the complaint, HRDC apologized to the individuals, re-sent to them the information that had been misdirected and revised its mailing procedures to minimize the chances of a reoccurrence.

Unauthorized disclosure of a SIN

We investigated an individual's complaint that Human Resources Development Canada (HRDC) improperly disclosed his social insurance number (SIN) to a private investigator.

The complainant had filed a lawsuit against an insurance company that he believed had mishandled his insurance claim. During the court process he discovered that the insurance company had hired a private investigator to delve into his financial affairs. He obtained a copy of the investigator's report, and noted references to inquiries conducted at HRDC, and the information obtained as a result of those inquiries. Dissatisfied because of HRDC's apparent lack of willingness to address his concerns about this breach of his privacy, the individual eventually turned to this Office for assistance.

We established during the investigation that an employee of HRDC had queried the complainant's file in the Social Insurance Register (SIR) system during the same time period that the private investigator had conducted his inquiries. Although the complainant reported his concerns to HRDC, it did

not pursue the matter further until he indicated that he intended to subpoena HRDC employees to testify in court in his suit against the insurance company. At that time he asked for a copy of HRDC's investigation file concerning the disclosure of his SIN and any information related to the action taken by HRDC in that regard. It was only at this point – almost ten months after he first reported his concerns – that HRDC decided to conduct an internal inquiry to determine whether, or how, his SIN may have been compromised.

*Dissatisfied because of
HRDC's apparent lack
of willingness to address
his concerns about this
breach of his privacy,
the individual
eventually turned to this
Office for assistance.*

It was clear from the evidence obtained during our investigation that the HRDC employee had obtained access to the individual's SIN without justification and disclosed it to the private investigator. The evidence also pointed to the possibility that the employee had also gained access to approximately 40 other client files on the SIR system for which there were no related HRDC case files that would require the employee to query their SIN files.

The former Commissioner was concerned with HRDC's lack of conviction in handling the individual's complaint about the disclosure of his SIN when he first brought it to their attention. They failed to take any action other than to issue him a new SIN, despite the fact that several officials were aware of the incident long before he complained to this Office. The former Commissioner was equally concerned that despite the seemingly adequate systems capabilities, HRDC managers do not routinely monitor the SIR system to identify and deal with any activities of a suspicious nature or that cannot otherwise be justified as part of an employee's duties.

The former Commissioner concluded that HRDC was responsible for its employee's improper disclosure of the individual's SIN to the private investigator, and that it had as a result contravened the confidentiality provisions of the *Privacy Act*.

In response to this finding, HRDC undertook to mitigate the damage to the extent possible. The Deputy Minister sent a letter of apology to the complainant, and implemented measures that will significantly enhance the security of personal information in the SIR database, and enhance monitoring of employees' access to the SIR. We are confident that this will improve HRDC's abilities to protect the personal information under its control and prevent any further violations of client privacy.

HRDC also decided to refer the matter to the Royal Canadian Mounted Police for criminal investigation – the employee was eventually fired by HRDC for the breach of security.

Statistics Canada census taker not responsible for disclosing personal information to banks

An individual alleged that Statistics Canada sold her name and address to financial institutions that then sent her unsolicited mail. The individual travelled frequently for extended periods and maintained a post office box. She was staying at a recreation vehicle park at the time of the 2001 census and the census taker explained to the individual that she would have to use the park address for the purposes of the census, which she did. Within a couple of months, she began to receive unsolicited mail addressed to her at the park. As she had only used that address for the census, it seemed logical to her that Statistics Canada must have sold or otherwise provided the address to the financial institutions.

We examined one solicitation that the individual had received and contacted the bank that had sent it to her. Using the code displayed on the form letter, the bank was able to determine that it had obtained her name and park address from one of the largest list management companies in Canada, which

handles more than 500 mailing lists representing some 25 million names. Its officials confirmed that the complainant's information was contained on one of the mailing lists which had been created and updated from information obtained from provincial telephone companies across Canada.

This detail prompted the individual to recall that she had a telephone installed at the park. While her telephone bill was sent to her post office box address, she had to provide the telephone company with the address of the park in order to have the telephone installed and serviced. It became apparent that it was the telephone company and not Statistics Canada that had disclosed the individual's name and address to the list broker, which in turn provided her information to the banks.

During the investigation, the list broker was asked to remove the individual's name from the mailing list, which it did immediately. However, the individual was alerted to the possibility that while her name would not be on an updated list, old lists held by the list broker's customers might still contain her information, and thus she might continue to receive solicitations. The former Commissioner urged her to contact those companies directly in order to remove her name from those lists. He also reminded the complainant that her name could be included in other lists in the future if, for example, she applies for credit cards, completes contest forms or purchases magazine subscriptions.

Time Limit Complaints

Under the *Privacy Act*, Canadians have a right of access to their personal information held by Government institutions and, by law, institutions must respond within 30 days after the request is received. Institutions can, however, extend that time limit to a maximum of an additional 30 days, but only under two specific circumstances: if meeting the 30-day time limit would unreasonably interfere with the institution's operations, or if consultations are required which cannot reasonably be completed within that time.

The number of complaints related to time limits being exceeded by federal institutions for providing personal information to citizens increased to 541

this year, compared to the 428 that were reported for the previous fiscal year. We closed 381 of these complaints, of which 302 were well-founded.

There were more complaints about the personal information-handling practices of Correctional Service Canada (CSC) than any other federal Government institution. Of the 177 complaints against CSC that we completed, 159 were well-founded. Although CSC increased its staff and streamlined its procedures, a delay problem in responding to requests for personal information continues.

The number of time limit complaints against two institutions dropped significantly in comparison to last year, whereas those against four others increased:

Canada Customs and Revenue Agency:	down from 85 to 31
Human Resources Development Canada:	down from 57 to 16
Correctional Service Canada:	up from 125 to 233
Royal Canadian Mounted Police:	up from 16 to 71
Department of National Defence:	up from 35 to 58
Citizenship and Immigration Canada:	up from 40 to 49

One factor that continues to hamper the ability of institutions to respond to requests within the prescribed time limits is the complexity of processing audio and videotapes.

Institutions sometimes record interviews conducted for administrative or criminal investigations. Since the *Privacy Act* applies to personal information that is "recorded in any form," individuals can ask for copies of their information on those tapes. It is a time-consuming process to listen or view tapes and then to identify and sever the information that requesters are not entitled to receive, often because it constitutes personal information about other individuals. The Department of National Defence is one of the organizations that records interviews, and it has recently acquired new equipment in an attempt to simplify the process of reviewing and severing information on tape.

Requests for voluminous investigation files also account for some delays in responding in a timely manner.

Transmittal of information by fax

Although we discourage institutions from sending personal information by fax, we realize that they are used regularly by institutions for the purposes of expediency in getting information to its destination.

One of our investigations uncovered a problem with the manner in which a Government institution was keeping a record of the personal information it was sending by fax. Fax cover sheets indicated the number of pages sent, to whom, by whom and on what date, but the institution could not identify, after the fact, which specific documents or pages had been transmitted. In other cases, the institution was not able to identify what it had received by fax from other areas in the institution.

It is imperative that institutions keep a record of the use and disclosure of personal information under their control. Except in limited circumstances, individuals have the right to know which documents containing their personal information are sent to whom and why they are disclosed.

A solution to this problem is to list the documents sent or received on the transmittal cover sheet itself. This will ensure transparency, document the flow of information and assist us in our investigations.

Processing original files versus photocopies

Some Government institutions have denied individuals access to their personal information, thus contributing to the rising number of complaints to this Office, because the departmental Access to Information and Privacy (ATIP) offices are increasingly relying on photocopies provided by their program areas, rather than working with original documents, when processing requests. The problem with this arrangement is that ATIP analysts cannot be certain that what they are given represents all the information the individual is seeking.

When this Office receives a "denial of access" complaint, we ask to see the original file to compare it with the information processed by the ATIP office. Often we have discovered that the ATIP office did not have all the information contained on the original file-because someone did not think it was relevant or had removed internal notes, or simply because the backside of double-sided documents had been missed when the documents were photocopied.

The subtle nuances that can only be appreciated when viewing original files are also lost. Photocopies do not reveal the use or meaning of different coloured forms or highlighting of significant passages, and may not capture the exact placement of post-it notes with comments. Nor do they include the paperclips that explain why certain documents are grouped together or why they are out of chronological order. These elements are essential to understanding the context of the file and to decide whether the personal information can be released to the individual.

Having our investigators review original files eliminates any misgivings that the institution may not have located all the requested information, and also gives us the unequivocal certainty that we require to ensure access has not been denied.

Although some program areas would rather not surrender their original files, particularly those with ongoing administrative activities, we suggest that they retain a photocopy for their own use for the few days it takes the ATIP office to review the original file. We also urge ATIP co-ordinators to reclaim their responsibility for the quality of responses they send to individuals by working with original files only.

INCIDENTS UNDER THE *PRIVACY ACT*

Incidents of mismanagement of personal information that warrant further review by this Office are sometimes brought to our attention. We conducted 32 such reviews last year.

As an example, last summer, following an office relocation from one building to another in Ottawa, Human Resources Development Canada's (HRDC) Disability and Benefits Appeal Branch staff discovered that two computers were missing. Although HRDC, following an investigation by its Security Division, was unable to determine exactly what had happened, it is believed that the computers were stolen when they were left unattended while waiting to be loaded into the moving trucks. It has been suggested that since both computers were new, they were taken because of their monetary value and not for what they contained. The theft was also reported to local police, but they were unable to find the missing computers or the perpetrators.

Our investigators ascertained that the computers had not been packed in boxes, but simply placed on moving trolleys without being secured in any way. They also determined that one HRDC employee was responsible for ensuring that all items were removed from their original location to the loading area, but no one actually supervised the physical transfer of items from that location to the moving trucks parked outside the building.

Although the computers were never found, HRDC was able to determine, by means of back-up computer tapes, that they contained the full names, social insurance numbers (SINs) and medical information of dozens of Canada Pension Plan (CPP) disability benefits recipients. Therefore, HRDC decided to notify those recipients about the theft.

During our review of the incident, however, we noted that an additional 38 individuals whose surnames and SINs appeared on documents had not been notified. Since this would be sufficient personal information to possibly identify these individuals, we asked HRDC to notify them of the theft as well, which it did.

We also recommended that HRDC implement additional security measures to ensure that this does not reoccur, specifically that it ensure that all personal information is removed from hard drives of computers before they are moved from one location to another; and that additional staff be present during moves to ensure adequate security for any personal information that is affected by the move.

In another incident, an individual informed this Office that documents he received from a small claims court relating to his suit against a Port Authority included personal information relating to other individuals, specifically their credit card account numbers.

Our staff determined that when the Port Authority filed its Statement of Defence in small claims court, it included a copy of a daily cash and deposit report and a cash deposit receipt. These documents identified other individuals along with their account numbers, invoice numbers, credit card numbers, and amounts paid to the Port Authority.

In its defence, the Port Authority believed that it had no choice but to file complete, unvetted documents with its Statement of Defence to comply with court procedures. As part of its defence it needed to present the information relevant to its financial transactions with the plaintiff, and was under the impression that it could not remove any information relating to the other individuals named in those documents.

When this Office made inquiries with the small claims court, we learned that it would in fact accept partial or severed documents. The Port Authority therefore could have removed all information not relating to the plaintiff when it filed its documents in court, including the personal information about the other individuals. We brought this matter to the attention of the Port Authority and, as a result, it has undertaken to have the information relating to the other individuals removed from the court's file. The Port Authority also contacted the concerned individuals to advise them that their personal information was included in a public record.

PUBLIC INTEREST DISCLOSURES

Paragraph 8(2)(m) of the *Privacy Act* allows the head of a Government institution to disclose personal information without an individual's knowledge or consent if there is a clear overriding public interest in doing so – either because it outweighs the individual's right to privacy or because it would clearly benefit the individual. Under section 8(5) of the *Act*, the Privacy Commissioner is to be notified in advance of any proposed disclosures.

This past year, the former Commissioner reminded a couple of institutions, following a review of their notifications, that the discretion to disclose personal information in the public interest should occur on an exceptional basis, where the disclosure cannot be justified under any of the other permissible disclosure provisions found in the *Act*.

It had become increasingly evident that some institutions were using the provision on a systematic and routine basis, with little apparent thought as to whether there was indeed an overriding public interest at the time. This was troubling because the situation seemed to play little or no part in the decision-making process. Often there had been no evaluation to assess what was of public interest and whether that interest should override the individual's privacy rights. As an individual rarely, if ever, has a chance to challenge the decision, it is critical that the decision-makers act in a judicious manner and ensure they have all the relevant information before making a fair determination.

However, of the 70 public interest disclosure notifications we received during the year, one was clearly warranted: the decision of the Department of National Defence (DND) to share with Veterans Affairs information regarding approximately 2,500 individuals involved in chemical warfare experiments.

From World War II to 1992, Defence Research and Development Canada (DRDC), a branch of DND formerly known as the Defence Research Establishment, compiled a list of DND members it had exposed to various

chemicals as part of its chemical warfare research program. The members were volunteers, but some may not have been aware they were part of the experiments.

As a result of a recent investigation by the Office of the Military Ombudsman, DND felt that the DRDC's information would be useful to Veterans Affairs in identifying veterans who could be entitled to benefits. The information included the individual's last name and initials, the name of the chemical administered, the date administered and the location. It also included some service numbers but no dates of birth, which left it impossible for DND to positively match all of the individuals to its employee records.

The DRDC had not copied this information to the service or medical files of the affected employees, and DND hoped that Veterans Affairs would compare the information with its records to identify any matches in its inventory, and get in touch with the individuals. The intent was that Veterans Affairs could review the cases of those veterans who claimed to have been exposed to noxious substances, including anthrax, but were refused financial assistance because there was no evidence on their service or medical files to support their claims.

The former Commissioner readily agreed with DND's decision. The benefit to the individuals was evident-Veterans Affairs could help to resolve benefit entitlement issues as well as to assist in the diagnosis and treatment of disease resulting from exposure to toxic substances.

Top Ten Departments by Complaints Received

April 1, 2002 to March 31, 2003

Organization	Total	Access to Personal Information	Time	Privacy	Other
Correctional Service of Canada	456	106	233	117	0
Canada Customs and Revenue Agency	205	127	31	47	0
Royal Canadian Mounted Police	200	101	71	28	0
National Defence	130	51	58	21	0
Citizenship and Immigration Canada	107	52	49	6	0
Human Resources Development Canada	85	38	16	31	0
Canada Post Corporation	71	37	13	21	0
Justice Canada	65	47	13	5	0
Canadian Security Intelligence Service	57	48	8	1	0
Canadian Nuclear Safety Commission	36	1	0	35	0
Others	230	100	50	80	0
Total	1,642	708	542	392	0

Completed Investigations and Results by Department

April 1, 2002 to March 31, 2003

Organization	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discontinued	Resolved	Settled	Total
Agriculture and Agri-Food Canada	2	1	1	2	0	5	11
Canada Customs and Revenue Agency	37	14	878	6	8	46	989
Canada Mortgage and Housing Corporation	0	0	0	0	0	2	2
Canada Post Corporation	17	4	11	6	0	8	46
Canadian Heritage	0	0	1	0	0	0	1
Canadian Human Rights Commission	0	0	1	0	0	0	1
Canadian International Development Agency	1	0	1	0	0	0	2
Canadian Nuclear Safety Commission	0	0	35	1	0	0	36
Canadian Security Intelligence Service	5	2	18	0	1	0	26
Canadian Space Agency	2	0	0	0	0	0	2
Citizenship and Immigration Canada	33	4	28	13	0	28	106
Commission for Public Complaints against the RCMP	0	0	5	0	0	0	5

Completed Investigations and Results by Department (continued)

April 1, 2002 to March 31, 2003

Organization	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discontinued	Resolved	Settled	Total
Correctional Service of Canada	189	17	42	11	1	65	325
Environment Canada	0	1	2	3	0	0	6
Farm Credit Corporation Canada	1	0	0	0	0	1	2
Finance Canada	0	1	0	0	0	0	1
Fisheries and Oceans Canada	1	3	4	1	0	0	9
Foreign Affairs and International Trade Canada	0	0	5	0	0	0	5
Freshwater Fish Marketing Corporation	0	1	0	0	0	0	1
Health Canada	2	1	6	1	0	1	11
Human Resources Development Canada	19	7	1,568	6	2	6	1,608
Immigration and Refugee Board	4	4	13	0	0	1	22
Indian and Northern Affairs Canada	1	0	2	0	0	3	6
Industry Canada	0	0	1	0	0	1	2
Inspector General of the CSIS	0	0	2	0	0	0	2
Justice Canada	4	1	11	1	0	7	24
National Archives of Canada	1	0	1	1	0	3	6

Completed Investigations and Results by Department (continued)*April 1, 2002 to March 31, 2003*

Organization	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discontinued	Resolved	Settled	Total
National Defence	25	7	10	7	1	14	64
National Parole Board	0	0	1	1	0	3	5
Office of the Chief Electoral Officer	0	0	0	1	0	0	1
Office of the Commissioner of Official Languages	0	1	0	0	0	1	2
Privy Council Office	0	1	5	0	0	0	6
Public Service Commission of Canada	1	0	2	0	0	1	4
Public Works and Government Services Canada	3	0	0	0	0	3	6
Royal Canadian Mounted Police	20	5	41	12	0	28	106
Solicitor General Canada	0	0	6	0	0	0	6
Statistics Canada	0	0	6	0	0	6	12
Transport Canada	1	2	0	2	0	1	6
Treasury Board of Canada Secretariat	0	0	2	0	0	0	2
Vancouver Port Authority	0	0	0	1	0	0	1
Veterans Affairs Canada	2	0	2	0	0	1	5
Total	371	77	2,711	76	13	235	3,483

Completed Investigations by Grounds and Results*April 1, 2002 to March 31, 2003*

	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discontinued	Resolved	Settled	Total
Access to Personal Information	14	72	228	36	5	131	486
Access	14	71	221	33	5	129	473
Correction/ Notation	0	1	7	3	0	0	11
Language	0	0	0	0	0	2	2
Inappropriate Fees	0	0	0	0	0	0	0
Privacy	56	4	2,445	17	8	86	2,616
Collection	7	2	831	2	7	19	868
Retention and Disposal	4	0	4	0	0	13	21
Use and Disclosure	45	2	1,610	15	1	54	1,727
Time Limits	301	1	38	23	0	18	381
Correction/Time	2	0	0	0	0	0	2
Time Limits	287	1	29	23	0	18	358
Extension Notice	12	0	9	0	0	0	21
Other	0	0	0	0	0	0	0
Total	371	77	2,711	76	13	235	3,483

Origin of Completed Investigations

April 1, 2002 to March 31, 2003

Province/Territory	Number
Newfoundland	14
Prince Edward Island	3
Nova Scotia	59
New Brunswick	52
Quebec	2,247
National Capital Region—Quebec	22
National Capital Region—Ontario	96
Ontario	396
Manitoba	83
Saskatchewan	55
Alberta	167
British Columbia	273
Nunavut	0
Northwest Territories	0
Yukon	4
International	12
Total	3,483

Inquiries under the *Privacy Act*

April 1, 2002 to March 31, 2003: 5,183

We will attempt to provide a breakdown of these inquiries by subject in future Annual Reports.

PRIVACY PRACTICES AND REVIEWS

Section 37 of the *Privacy Act* empowers the Commissioner to initiate compliance reviews of the personal information management policies and practices of federal institutions. This means that, at the Commissioner's discretion, he can audit them to determine whether they adhere to the fair information practices set out in sections 4 to 8 of the *Act*. The Privacy Practices and Reviews (PP&R) Branch may evaluate the compliance of organizations with the requirements of the *Privacy Act*.

In the aftermath of September 11, 2001, a number of federal Government departments and agencies received significant funding increases to allow them to implement changes to combat terrorism and enhance national security. To assess the impact that these anti-terrorism measures are having on individual privacy, the Office initiated reviews of the personal information handling practices at the Royal Canadian Mounted Police, the Canadian Security Intelligence Service and the Communications Security Establishment. The reviews will be completed in the upcoming fiscal year.

A number of programs and activities established by federal Government institutions and agencies provide for the disclosure of personal information about Canadian citizens and residents to departments and agencies of the United States government. During this fiscal year, the Office initiated an examination of agreements, arrangements and memoranda of understanding between Canada and the United States that include provisions for the sharing of personal information. Eighteen departments and agencies were selected for this examination and a review will be completed in the upcoming fiscal year.

In addition to reviewing and auditing, our Office advises federal organizations on compliance issues and the privacy implications of new and existing programs and practices. The Office's PP&R Branch has been involved in numerous consultative efforts with Government departments, including the Treasury Board of Canada Secretariat, Elections Canada, Statistics Canada, Human Resources Development Canada, Indian and Northern Affairs Canada, and Health Canada, to name a few.

These consultations often involve reviewing new information management proposals, such as data-matching initiatives, the creation of databases and information-sharing arrangements with other organizations. It is important to note that the Commissioner's role in such issues is an advisory one. The Commissioner does not in any way provide formal approval for such initiatives, which would compromise his impartiality during subsequent investigations or reviews.

As described in our earlier reports, HRDC developed a review procedure to deal with policy analysis, research and evaluation activities involving the linking of separate databanks. Part of this procedure includes consultation with our Office. During the past year, the Office has analyzed and commented on close to a dozen HRDC submissions, including the Evaluation of HRDC Work Sharing Program, the Evaluation of Labour Market Information Services, and the Canada Student Loan Program Needs Assessment and Loans Disbursement Datasets Project.

One project that the department sent our Office, the Employer and Industry Activity System, was submitted as an undertaking involving databank connections. Upon review, our Office concluded that the project involved more than simply the linking of existing databanks. Rather, it would result in the creation of a new databank that would be used on an ongoing basis. It was never contemplated that this type of project would be dealt with through this process. As a result, we advised HRDC that the matter would be more appropriately dealt with by way of a Privacy Impact Assessment (PIA), which entails a more rigorous review. PIAs are discussed in more detail in the following section of this Report.

We have continued to notice an improvement in the detail and completeness with which HRDC's submissions address privacy issues. In our last Report, we expressed a concern that HRDC provided limited information regarding contracts with outside parties, and we said that HRDC should strengthen the contractual obligation of those parties to protect the privacy of personal information under their temporary stewardship. Although some of the submissions we received did not fully meet expectations, the department has improved in addressing this concern over the past year.

PRIVACY IMPACT ASSESSMENTS

On May 2, 2002, the Secretariat of the Treasury Board of Canada issued a new directive requiring federal Government departments and agencies to undertake a Privacy Impact Assessment (PIA) for all new programs or services that raise privacy issues. Canada is the first country in the world to make PIAs mandatory for all federal departments and agencies.

For more than a year prior to that date, the Office had been urging the Government to put a PIA Policy in place, in order to ensure that privacy considerations are built in at the outset of projects and not as an afterthought. In developing this Policy, we congratulate the Government for implementing the Policy and for recognizing that respect for citizens' privacy is critical to the success of all its programs and services, including the Government On-Line initiative.

New and existing programs and services with potential privacy risks must now undergo a PIA – in effect, a feasibility study from a privacy perspective. This includes significant redesigns of existing programs when the redesign involves a new or increased collection, use or disclosure of personal information, new data-matching, contracting-out or other changes that potentially raise new privacy concerns.

A PIA is designed to provide federal Government departments and agencies with a consistent framework to forecast a proposal's impacts on privacy, assess its compliance with privacy legislation and principles, and determine what mitigating measures are required to overcome the negative impacts. If done correctly, a PIA is a way to avoid extra costs, adverse publicity, and the loss of credibility and public confidence that could result from a proposal that is not privacy friendly. It is also a way to raise awareness and understanding of privacy principles, both internally and among citizens.

The conduct of a PIA is a shared responsibility. As the Treasury Board Policy states, PIAs are co-operative endeavours, requiring a variety of skill sets, including those of program managers, technical specialists, and privacy and

legal advisors. Although the deputy head of a federal institution, department, or agency is responsible for determining if a PIA is required, several Government departments have set up internal committees to review departmental projects to determine whether a PIA is required. Given the multi-disciplinary nature of the exercise, this strikes us as a sensible approach.

Of particular significance is the fact that the Policy requires departments to inform the Office of all proposals for new or modified programs and services that raise privacy issues. Departments must also consult the Office while preparing a PIA to ensure that privacy risks are identified and that mitigating actions to deal with those risks are appropriate. By reviewing the documentation in cooperation with institutional officials, our Office is then able to provide advice and guidance to institutions and identify solutions to potential privacy risks.

The Commissioner's role is not to approve or reject projects that are assessed in the PIAs, but rather to assess whether or not departments have done a good job of evaluating the privacy impact of a project or proposal.

To take on this new responsibility, we created a new division within the PP&R Branch devoted entirely to analyzing and providing comments on PIAs submitted for review.

During the period of this Report, our Office received 17 PIAs and 12 preliminary PIAs (PPIAs), and has been consulted on several projects that would require PIAs. Based on discussions with the Treasury Board Secretariat (TBS) and other federal Government departments and agencies, we expect to receive more than 50 PIAs over the next fiscal year.

Most of these initiatives or projects involve the electronic delivery of services to individuals through the Internet, so the privacy risks come from a variety of sources, including systems characteristics, technical infrastructure and design of the on-line service or program.

Five of the 17 PIAs we received were prepared prior to the TBS Policy being introduced, and thus did not adhere to the policy requirements or the guide-

lines associated with the Policy. As a consequence, most were either returned to or withdrawn by the submitting departments to be revised in accordance with the Policy. So far, eight PIAs received have run the full course of the review process.

While the majority of reports received to date from departments are PIAs, we have witnessed over the course of the year a growing number of Preliminary Privacy Impact Assessments (PPIAs). We believe this trend reflects an inclination on the part of departments to adopt a more cautious and phased approach to the develop-

ment of their PIAs, given their unfamiliarity with the process and the probable lack of in-house expertise in this area. Where departments are facing a fixed and impending deadline for implementation, we have been advising those departments to directly draft their PIA to expedite the review process.

So far there has been no PIA, and certainly no PPIA, where our staff has not found it necessary to go back to the submitting department for additional information. Some commonly omitted elements include:

- a project implementation schedule;
- a complete inventory of data elements collected and used (information may be described, but not itemized);
- an adequate description of the business process;
- a data flow chart, or one that is complete; and
- an adequate description of the information security infrastructure associated with the project.

The Commissioner's role is not to approve or reject projects that are assessed in the PIAs, but rather to assess whether or not departments have done a good job of evaluating the privacy impact of a project or proposal.

In addition to this, background documents commonly missing include:

- draft agreements, where third party service providers are involved;
- Threat and Risk Assessment (TRA) reports, where conducted;
- project feasibility studies, where conducted;
- project management plans, as they relate to project design; and
- technical specifications relating to system design.

There are also a number of common problems which we have observed in the privacy analysis. They include:

- confusing privacy with security and confidentiality;
- seeing the PIA process as essentially a privacy compliance audit exercise;
- failure to link identified risks with specific design elements of the project;
- proposed mitigating measures not addressing the risk identified; and
- proposed mitigating measures for risks that have not yet been identified.

Although these problems and omissions reflect the unfamiliarity of departments with the PIA Policy, it should be noted that we are now beginning to see a general improvement in the quality of the PIAs we are receiving.

If there are lessons to be drawn from our experience of the last eleven months, one is the need for greater education on how the PIA functions as a risk management tool. Another is the need for departments to notify and involve the Office at the earliest possible stage in the development of the PIA.

Given that there is a need for organizations to have a better understanding of the PIA Policy, we advise Government officials to contact the Treasury Board Secretariat or to visit its Web site at www.tbs-sct.gc.ca for more information.

IN THE COURTS

Section 41 of the *Privacy Act* allows an individual, following the results of an investigation of a complaint by the Privacy Commissioner, to apply to the Federal Court for review of the decision of a Government institution to refuse the individual access to her personal information. From the time the *Privacy Act* came into force in 1983 to March 31, 2003, approximately 130 applications for review have been filed in the Federal Court. Eight of these were filed in the year ending March 31, 2003.

Section 42 of the *Privacy Act* allows the Commissioner to appear in Federal Court. The Commissioner can apply to the Federal Court for review of the decision of a Government institution to refuse access to personal information if he has the consent of the individual who requested the information. The Commissioner can appear before the court on behalf of an individual who has applied for review under section 41. Or, with leave of the court, he can appear as a party to any review applied for under section 41.

There are currently no applications under the *Privacy Act* in which the Commissioner is actively involved. However, the Commissioner also participates in litigation that arises outside of the *Privacy Act*. Following is a summary of litigation involving significant privacy issues in which the Commissioner has been involved.

Mertie Anne Beatty et al. v. The Chief Statistician et al.

Federal Court File No. T-178-02

This issue was brought before the Federal Court of Canada by a group of Canadian citizens seeking access to the 1906 Census Returns for the Provinces of Manitoba, Saskatchewan and Alberta pursuant to section 6 of the Privacy Regulations.

The Offices's position has always been that disclosure of the 1906 census information is prohibited by the confidentiality provisions in the *Statistics Act*, and that legislative amendments should, therefore, be explored as a means of compromise.

Status

The Application was filed in February 2002. Following a review of the legislation, the federal Government decided that the information could, in fact, be released and did so. Bill S-13 was later introduced in order to retroactively modify census laws to allow access to records and address privacy concerns. Accordingly, the Application was discontinued.

Canada Post Corporation v. Privacy Commissioner of Canada

Federal Court File No. T-233-02

On January 14, 2002, the former Commissioner determined that Canada Post's use of its National Change of Address (NCOA) service contravened the *Privacy Act* in two ways. First, Canada Post contravened section 5(2) of the *Act* by failing to specify to NCOA applicants its intention to disclose new addresses to mass mailers and direct marketers for a commercial purpose. Then it contravened section 8 by failing to obtain the consent of individuals for the disclosure of their new addresses to mass mailers and direct marketers.

Status

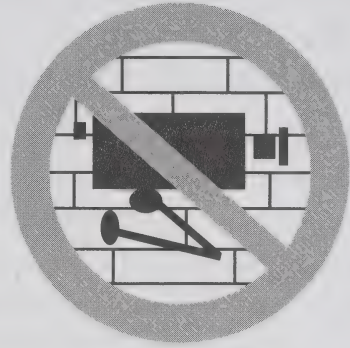
On February 13, 2002 Canada Post filed an Application alleging that the former Commissioner had exceeded his jurisdiction in applying sections 5 and 8 of the *Privacy Act*. On April 4, 2002, however, Canada Post agreed to add a box on its form enabling individuals to provide consent for this activity. The issue thus became moot, and Canada Post discontinued its Application on April 14, 2002.

Privacy Commissioner of Canada v. Attorney General (Canada) et al.

British Columbia Supreme Court File No. S57566

In June 2001 the Office received a complaint regarding the installation of Royal Canadian Mounted Police (RCMP) surveillance cameras in the downtown core of the City of Kelowna, B.C. After an investigation, the former Commissioner determined that by recording continuously rather than recording only selective incidents related to law enforcement activities, the

RCMP is unnecessarily collecting information on thousands of innocent citizens engaged in activities irrelevant to the mandate of the RCMP. It was concluded, therefore, that the video surveillance in Kelowna was in contravention of the *Privacy Act*.



The RCMP informed this Office that the continuous video recording of the surveillance camera was terminated on August 28, 2001. Instead, the area under surveillance would only be videotaped if a violation of the law was detected. While this put the use of the surveillance camera into compliance with the letter of the *Privacy Act*, which technically only applies to information that is “recorded in any form”, it was the former Commissioner’s opinion that a continuation of the video camera surveillance even without continuous recording was insufficiently respectful of the spirit of the *Privacy Act* and of the privacy rights of Canadians.

On June 21, 2002, the former Commissioner filed a Statement of Claim in the Supreme Court of British Columbia, requesting declarations from the Court that this generalized video surveillance was unconstitutional, contravening the *Charter*, as well as Canada’s international human rights obligations. From March 12 to 14, 2003 there was a hearing on the federal Government’s motion to dismiss the case. The court held that the Commissioner lacked the legal capacity to bring the action.

Status

On July 4, 2003, the newly-appointed Commissioner announced that he had instructed counsel to withdraw its appeal into the case. Although the Commissioner and this Office continue to have a variety of concerns regarding video surveillance of public places by public authorities, continuing this particular action was not perceived as a useful way of spending public funds.

Information Commissioner of Canada v. Commissioner of the RCMP et al.

Supreme Court of Canada File No. 28601

A list of the career postings of four Royal Canada Mounted Police (RCMP) officers was requested under the *Access to Information Act*. The Commissioner of the RCMP refused to release the information on the grounds that it revealed employment history and thus was personal information as defined in section 3 of the *Privacy Act*. The Information Commissioner argued, however, that paragraph 3(j) of the definition of personal information in the *Privacy Act* states that information relating to the position or functions of Government officers or employees is not personal information for the purposes of section 19 of the *Access to Information Act*.

Status

The Supreme Court of Canada released their unanimous decision on March 6, 2003. The Court very clearly stated that information may be personal and yet still fall under the rubric of section 3(j) where it reveals general characteristics associated with the position or functions held by an officer or employee of a federal institution. The Supreme Court felt that none of the information requested pertained to the competence or characteristics of the employees. It therefore ordered that the following information be released for each of the named individuals: a list of historical postings, status and dates, a list of ranks and dates those ranks were achieved, and the years of service and anniversary date of service.

The decision of the Supreme Court limits the application of paragraph 3(j) of the definition. Even though this Office had argued for a narrower interpretation of the exception, the decision of the Supreme Court is not unreasonable.

Part Two

Report on the *Personal Information Protection and Electronic Documents Act*

INTRODUCTION

The *Personal Information Protection and Electronic Documents (PIPED) Act* sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

Since the *Act* took effect on January 1, 2001 it has applied mainly to the commercial activities of what are known as federal works, undertakings or businesses, such as transportation and telecommunications companies, banks and broadcasters. It also applies to the personal information of employees in those companies, and it applies to personal information that is sold, leased, or bartered across provincial or national boundaries by provincially-regulated organizations. As of January 1, 2002, the personal health information collected, used or disclosed by these organizations is also covered. On January 1, 2004, the *PIPED Act* will cover the collection, use or disclosure of personal information in the course of all commercial activities in Canada, except in provinces which have enacted legislation that is deemed to be substantially similar to the federal law.

The second full year under the *PIPED Act* proved to be an interesting and challenging one for our Office on several fronts. We began to accept and investigate complaints that concern the personal health information of individuals. We also made further inroads into a myriad of issues, including consent and marketing, credit scoring, the recording of telephone calls and security clearances.

We also undertook a number of communications activities to raise awareness of privacy issues and federal privacy laws. From April 1, 2002 to March 31, 2003 the former Commissioner and senior staff delivered 49 speeches at conferences and special events; we issued more than 25 news releases and media advisories on key privacy issues; we responded to hundreds of media requests for information and interviews; we disseminated more than 23,000 of our publications to members of the public, businesses and other organizations across the country; and we received an ever-increasing number of hits to the Web site, averaging approximately 50,000 hits per month.

The *PIPED Act* requires the Commissioner to submit an Annual Report to Parliament on the activities of the Office in the previous year. The current Report covers the period from January 1, 2002 to December 31, 2002 for the *PIPED Act*.

INVESTIGATIONS AND INQUIRIES

During the 2002 calendar year, the Office received 300 complaints under the *PIPED Act* from individuals alleging that their privacy rights had been violated by a wide range of different organizations. Approximately 37% of the cases dealt with practices in the banking sector, followed by 19% with the telecommunications and broadcasting sector, 15% with transportation companies, and 13% with the nuclear sector. The remaining complaints, 16%, were filed against a variety of other types of organizations, including Internet service providers, credit bureaus and aboriginal band councils.

The former Commissioner issued findings for 162 complaints under the *PIPED Act* in 2002 and they were concluded as follows:

Not well-founded	61
Well-founded	45
Resolved	41
Discontinued	15

In addition to this, the Office also conducted five incident investigations. Incidents are matters that the Commissioner becomes aware of from various sources, including the media. Usually a victim is not identified and a complaint has not been filed with the Office.

What follows in this Report is a sampling of some of the year's more notable cases. More detailed summaries of all findings under the *PIPED Act* are available on our Web site, at www.privcom.gc.ca. These findings are posted in order to provide guidance to organizations and the legal community on the application of the *Act*.

DEFINITIONS OF FINDINGS UNDER THE *PIPED ACT*

Not well-founded: This means that there is no evidence to lead the Privacy Commissioner to conclude that the organization violated the *Personal Information Protection and Electronic Documents (PIPED) Act*.

Well-founded: This means that the investigation revealed that the organization failed to respect a provision of the *Personal Information Protection and Electronic Documents (PIPED) Act*.

Resolved: This means that the organization has taken corrective action to remedy the situation, or that the complainant is satisfied with the results of the inquiries made by the Office of the Privacy Commissioner of Canada.

Discontinued: This category applies to investigations that are terminated before all the allegations have been fully investigated. A case may be discontinued for any number of reasons, such as the complainant no longer being interested in pursuing the matter.

SUMMARY OF SELECT CASES UNDER THE *PIPED ACT*

A case of mistaken identity

A complainant who wrote to the Office said she was notified by a friend that a notice in the newspaper indicated that the police were looking for her. To her horror, the complainant found herself looking at her own image in a photograph accompanying the Crime Stoppers "Crime of the Week" article. The article described a recent theft of two cheques from an elderly woman and identified the depicted person as a suspect in the crime. The image had been captured from a video surveillance camera at a bank. The camera had been pointed at the teller's wicket where the thief had cashed the stolen cheques.

As it turned out, the complainant had indeed visited the same bank and the same teller's wicket on the day in question, but not to cash a cheque. She had gone there simply to pay a bill. It was clear that she was not the actual perpetrator of the crime.

It was the same bank, the same wicket, the same day, but not, as our investigator learned, the same time.

On the day in question, the clock on the bank's journal roll (its computerized record of transactions) had been 12 minutes slower than the clock on the video camera. When the bank's security staff later forwarded the videotape to the time of the cheque-cashing as indicated by the journal roll, the image that appeared was not that of the actual cheque-casher. Rather, it was the image of the woman who had preceded the cheque-casher at the teller's wicket by some 12 minutes – the complainant.

Thus, the photographs that the bank subsequently gave to the local police, and the police in turn to the Crime Stoppers organization, depicted the wrong person.

A week after the original "Crime of the Week" article, Crime Stoppers ran a retraction in the same local newspaper. On the same day, the newspaper itself ran a front-page story, clarifying that the complainant had been a victim of mistaken identity. The complainant also received formal apologies from the bank, the police, and

Crime Stoppers. The two latter organizations further admitted that they had both failed to follow normal verification procedures, and both have since collaborated in instituting measures to prevent similar occurrences. The bank also instituted procedural changes to verify the time on surveillance tapes and journal rolls.

However, the complainant was not entirely satisfied. After her initial shock and distress, she became even more concerned about the effect the incident was having on her reputation when she learned that many people had indeed recognized her image from the article. This was of particular concern because her work depended upon her ability to visit clients' homes and offices. She was also concerned that her image may have appeared in other Crime Stoppers notices. Our Office was able to reassure the complainant that her photograph had been used in only the one newspaper article.

As to the disposition of her formal complaint to the former Commissioner, we considered the matter in relation to the bank's obligations under the *PIPED Act* to ensure the accuracy of personal information.

*To her horror, the
complainant found
herself looking at her
own image in a
photograph
accompanying the
Crime Stoppers "Crime
of the Week" article.*

We determined that the personal information at issue – the photograph of the complainant – had been wholly inaccurate in a situation where accuracy had been crucial to the purpose of solving a crime. On that account alone, the bank should have made sure that the information it disclosed was as accurate as possible. It had not done so, and therefore was in clear contravention of Principle 4.6 of the *Act*. In the letter of findings to the complainant, the former Commissioner wrote:

“ ... an organization must take due account of the potential adverse consequences of inaccurate information for the individual. I have determined that your personal information inaccurately disclosed by [the bank] was used to make a decision about you – specifically, an erroneous decision to the effect you were to be sought as a prime suspect in a crime. This was a decision, moreover, that caused you substantial notoriety, embarrassment, and worry about your reputation and your livelihood. Being well aware that the police would likely use your personal information to make a decision about your status as a suspect, the [bank] should have taken due care to ensure that the information was accurate so as to minimize the possibility of a wrong decision with adverse consequences for you.”

The former Commissioner determined that this complaint was well-founded.

U.S. security measures affect Canadian pilots

The aftermath of September 11, 2001 continues to be felt by average Canadians. One individual directly affected by new security measures, a commercial airline pilot, was confronted with a difficult choice: forfeit his privacy rights or risk losing his job. In the past, when he needed to take aircraft training required to keep his licence, his employer simply sent him to a flight school in Florida. This changed after the September 11 terrorist attacks. American flight schools were now obliged to have their foreign students – including Canadian commercial airline pilots – sign an authorization form. The form would allow the U.S. government to collect and disclose personal information about the students. However, it did not adequately explain the purposes for, nor did it appear to set any limits on, this collection and disclosure.

When his employer asked him to sign the form, the pilot was incensed. After all, he had already undergone an extensive background check by the Government of Canada. He disliked the prospect of a foreign government sifting through his background – especially when it was not clear what information would be collected and to whom it would be disclosed.

No one seemed comfortable with the form – the Canadian Government, the airline, the union – but there was no immediate solution on the horizon. The federal Government had asked the United States to accept Canadian background checks on commercial pilots. But at the time of the complaint, the United States had not yet made a decision.

The airline was troubled by the wording of the form, but was in a difficult situation. By law, its pilots require the training. The nearest alternative was a flight school in Europe – a more costly prospect than sending its pilots to Florida. Furthermore, since the pilot and co-pilot must train together, the airline would be in an awkward position if one pilot was willing to sign the form and the other was not.

The pilot's union protested the requirement to sign the form. It negotiated an agreement with the airline which stated, among other things, that the decision to sign the form was voluntary, and that the company would provide alternative training for dissenting pilots.

The pilot decided not to sign the form. Although his employer obtained a temporary extension of his licence until a resolution could be found, it did

*He disliked the prospect
of a foreign government
sifting through his
background – especially
when it was not clear
what information would
be collected and to
whom it would be
disclosed.*

not make alternative training arrangements for him. Unless the U.S. government agreed to Canada's request, or the former Privacy Commissioner made his findings, the airline was not going to change its decision. The pilot's extension eventually ran out.

We were highly critical of the authorization form. It was entirely objectionable on many fronts and we concluded that the practices it authorized completely failed to meet the fair information principles that are the cornerstone of Canada's privacy legislation.

In making these determinations, we relied on the "reasonable person test" outlined in section 5(3) of the *PIPED Act* to assess the airline's purposes. We acknowledged that, on the surface, the airline's reasons for making its pilots sign this form appeared reasonable. Below the surface, however, the purposes ceased to be acceptable. We thought very little of the airline putting cost and convenience ahead of the pilot's right to refuse consent to collection and disclosure practices that were clearly in contravention of Canadian law. It was noted that the airline had options but that it had chosen not to exercise them.

In finding that the airline's purposes did not meet the expectations of section 5(3), in the letter of findings, the former Commissioner commented on this timely example of the difficulty of balancing national security requirements with the fundamental right of privacy:

"I agree that the circumstances that many countries, most particularly the United States, currently find themselves in warrant some security measures. Of course it is reasonable to demand that pilots receive security clearance in order to fly, and that is why Canada has in place security measures that Canadian commercial pilots must undergo... But would a reasonable person consider it appropriate to require these same pilots to then consent to unacceptable collection and disclosure practices at the request of a foreign government? I think not. Indeed, I suspect most reasonable Canadians would find this encroachment on Canadian rights to be highly objectionable. Furthermore, most

Canadians would likely expect employers to provide reasonable options for employees and would demand that their government raise an alarm bell with the United States."

After receiving the letter of findings, the airline agreed with the former Commissioner's recommendation and arranged to provide training at an alternative location for the pilot and others who refuse to sign the form.

Bank's disclosure to individual's employer inappropriate

An individual went to his bank on personal business – to dispute a charge for cheques. He was not satisfied with the bank's response he was given and a scene ensued.

The branch manager came onto the scene and decided his staff should not have to deal any further with the customer. The firm that employed the customer happened to do a lot of important business with the bank. Before terminating the bank's relationship with the customer, the branch manager thought he should discuss the matter with the customer's employer.

The complainant was astounded when his employer confronted him about what had occurred at the bank earlier that morning.

One of our first tasks was to determine what exactly had been disclosed in the telephone conversation between the bank manager and the employer. In the absence of any evidence that they had discussed the complainant's financial affairs, it appeared that the actual disclosures about had been limited to three simple facts: (1) that he had an account with the branch; (2) that his account was to be terminated; and (3) that there had been a scene with the teller.

In the bank's view, none of this should have been considered the complainant's personal information. The bank pointed out that the scene itself had been acted out in a public place, and in a small community, where a person does his banking is hardly a matter of secrecy. The bank took the position that the disclosures in question fell into the category of "normal public discourse," comparable to "small-town gossip." The bank even suggested that it

had a right to make such disclosures for the sake of extending “business courtesy” and protecting its own business interests. Citing section 5(3) and Principle 4.3.5, the so-called “reasonableness” provisions of the *PIPED Act*, the bank also suggested that the complainant had not had a reasonable expectation of privacy, and that reasonable people would have considered the disclosures appropriate in the circumstances.

Although we were not unsympathetic to the bank and were willing to concede the reasonableness of the bank’s position up to a point, the former Commissioner had to draw the line somewhere. In the letter of findings to the complainant, the former Commissioner commented as follows:

“In my view, ... the reasonableness of the situation ends exactly at the point where the [bank] manager, in the full knowledge that you had been acting on your own behalf at his branch that morning, nevertheless picked up the telephone at his office during business hours to inform your employer. This was not casual or inadvertent disclosure. This was not small-town gossip. This was a deliberate act of disclosure of personal information to a third party by a person who was acting in an official capacity and who had no right to make such disclosure. Moreover, the Act puts the rights of individuals above such notions as ‘business courtesy’ and makes no distinction as to the size of one’s community. Would any reasonable person anywhere expect his bank manager to disclose information about his personal banking affairs to his employer? The answer to this question is obviously no.”

Credit score fraud

In the course of investigating complaints about credit reporting and scoring, we learned a great deal about the workings of the credit-granting industry at large.

In two particular cases, individuals had made formal requests under the *PIPED Act* for access to certain personal information on file with their banks. Specifically, each requester had wanted to know his credit score. The banks in question had refused access, each invoking the exemption provided in section 9(3)(b) of the *Act*. This provision says in effect that an organization does not

have to give access to personal information if doing so “would reveal confidential commercial information.”

The requesters, believing to the contrary that credit scores were personal information to which they were fully entitled to have access, filed complaints with the Office. Our main task in each case was to decide whether the exemption cited by the bank was valid.

A credit score is a numerical indication of credit-worthiness, generated by means of an algorithmic model. For most people familiar with the notion, the term “credit score” mainly conjures up the vision of credit-reporting agencies. These agencies are in the business of providing banks and other credit-granting institutions with background credit information, sometimes including credit scores, on prospective clients. In considering an application for credit, a credit-granting institution will often obtain the applicant’s credit history from a credit-reporting agency. In some cases, the institution will also request a credit score for the applicant. Credit-reporting agencies do not themselves generate credit scores, but rather provide scores that another company generates from the agency’s information.

Up to a point, the complainants had good grounds for their position. In prior cases, we had already considered the matter of access to personal credit information, at least as far as credit reporting agencies were concerned. We had already concluded that credit scores *are* personal information according to the definition in the *Act*, and that individuals *do* in principle have a right of access to them. We had determined that credit-reporting agencies in particular are required to comply with Principle 4.9 of the *Act* by giving individuals access on request to personal information in their credit files. We had fur-

*In the course of
investigating complaints
about credit reporting
and scoring, we learned
a great deal about
the workings of the
credit-granting industry
at large.*

ther determined that banks, if they have obtained an individual's credit information from a credit-reporting agency, must likewise give the individual access on request to the information, including any credit score provided by the agency.

But the more recent cases were not nearly as straightforward. The special problem they presented was that the credit scores sought by the complainants were not the usual agency-provided credit scores. They were in fact scores that the banks themselves had generated and assigned internally.

It is perhaps less widely known that banks, too, have credit scores, distinct from those provided by credit-reporting agencies. Banks generate their own internal credit scores by means of their own internal credit-scoring models, very different from those associated with agencies. Whereas agency scores are generated by means of standardized models based almost exclusively on credit information, a bank develops its own customized models, unique to the bank and incorporating not only credit information on the individual, but also many other elements pertaining to the bank's own strategic business priorities. Because banks regard and treat their internal credit-scoring models as proprietary confidential commercial information, such models are much more problematic in terms of the *Act*.

By citing section 9(3)(b), the banks in question were not suggesting that an internally generated credit score was itself confidential commercial information. Rather, they were saying that the model used to generate such a score was confidential commercial information. And they were saying in effect that internal credit scores, if made available to individuals, would reveal the model by which the scores had been generated.

*The special problem
they presented was that
the credit scores sought
by the complainants
were not the usual
agency-provided
credit scores.*

We accepted the banks' arguments that an internal credit-scoring model constituted confidential commercial information. But we were far less persuaded of the more crucial proposition – that releasing the credit scores would somehow reveal the credit-scoring model itself. How could merely letting a person know his credit score possibly lead to his knowing the inner workings of such a complicated, technical and algorithmic apparatus as a credit-scoring model?

As it turned out, it was not the average customer that the banks feared. It was fraudsters intent on “cracking” a bank's internal credit-scoring model for nefarious purposes. According to the banks, fraudsters could employ devious means to acquire a number of credit scores and then would extrapolate the model from the scores. Either the fraudsters would be working for the banks' credit competitors, trying to gain competitive advantage. Or they would be operating on their own behalf, trying to procure credit for themselves on false pretenses.

In their submissions to the Office, the banks presented an independent forensic analysis of the risk of fraud contingent upon the availability of credit scores. This analysis concluded that, if credit scores were readily available, the integrity of a bank's internal credit-scoring model could be compromised on the basis of a relatively small number of credit scores generated by the model.

The fraud scenarios outlined by the banks struck us as farfetched. To be fair, however, we sought the advice of an expert in the field of algorithms. This expert confirmed that access to customized credit scores would definitely make it easier to approximate a bank's internal credit-scoring model.

We were still doubtful. In particular, we were mindful that section 9(3)(b), by using the phrase “would reveal” rather than “could reveal”, set a very high standard for the withholding of personal information. On the word of the algorithm expert, we were willing to concede that a model could be approximated from knowledge of a certain number of scores, but we remained unpersuaded that it would ever happen. The banks' submissions had failed to convince us that fraudsters would actually go the lengths described to deceive a bank. We found it particularly difficult to accept the apprehension, evidently

shared by all banks, that even one's competitors in the credit-granting community would as a matter of course resort to such tactics in order to "crack" one another's models for the sake of competitive advantage.

Nevertheless, the fact remained that two banks had strongly expressed what we took to be genuine belief and fear that their internal credit-scoring models would inevitably be revealed and fraudulently manipulated if individuals were given access to credit scores. However unlikely it seemed to us, it was undeniably a prospect that the banks took very seriously. Moreover, it was a prospect that we were unable to wholly refute.

In the end, the former Commissioner decided to give the banks the benefit of the doubt. He did so primarily out of consideration for his responsibility to achieve a balance between the privacy rights of individuals and the legitimate informational interests of organizations. Seeing little informative value in a credit score on its own and no significant harm ensuing to Canadians' privacy rights from the inability to obtain internal credit scores, we thought it only fair in the circumstances to accept the banks' position.

The former Commissioner found that the banks had appropriately cited section 9(3)(b) to refuse the complainants access to their internal credit scores.

Customers beware: Your conversation may be recorded

The practice of taping customer telephone calls – common among many organizations – was the subject of two complaints. These cases illustrate two very different approaches taken by organizations to inform customers of the practice and obtain their consent. In both cases, as in those involving secondary marketing, reasonable expectations played a role in the former Commissioner's findings.

In the first case, an individual called his bank in the intended role of guarantor of his daughter's loan application. At the end of the conversation, he learned that his call had been tape-recorded. He had not been informed, either by the customer service representative or via a recorded message, that

his call would be taped. Nor was he asked, upon learning that the call had been recorded, if he agreed.

The bank had an interesting take on the issue of consent in this case. In its view, only one party had to consent to calls being recorded. It therefore required its customer service agents to sign a consent form for the taping of these calls.

The bank's purpose for recording the call was that it needed confirmation of the customer's records and evidence that the customer had consented to the product or service. In its view, the taped call is the equivalent of a signed form and is used for record-keeping purposes.

We agree that information exchanged during the conversation should be recorded in some way. However, the reasonable expectations of the customer should also be considered, and most individuals would want to know *beforehand* that their call is going to or may be taped. In this case, the bank clearly did not meet those expectations and did not have the father's consent to record his call, thus contravening the consent principle of the *PIPED Act*.

In the other complaint, an individual also alleged that his bank had recorded his telephone conversations without his knowledge and consent. This individual had taken the bank to court over liability for certain withdrawals made on his bankcard. During this process, the bank introduced a tape-recording of a telephone conversation between him and a bank employee.

The bank argued that it had this individual's consent to tape his calls. It referred to an agreement, signed by him when he opened his account, that acknowledged the bank's practice of recording telephone calls. There were also the privacy brochures given to him – five in all – which specified

*...most individuals
would want to know
beforehand that their
call is going to or
may be taped.*

the bank's purposes for collecting personal information. The complainant, however, did not read any of this information.

Then, there was a conversation between a bank employee and the complainant (also taped), in which the employee explained the bank's practice of recording conversations. To the complainant, "recording" did not necessarily mean electronic recording, and so he stood by his original complaint.

The former Commissioner determined that the bank had made a reasonable effort to inform the complainant of its practice and purpose and that it had his consent to record his calls by way of the agreement form that he had signed. We then found that the bank had complied with the relevant provisions of the *Act*.

Clearly, organizations such as this one, which have made the effort to inform customers and to obtain their consent, have the reasonable expectation that customers will read what is put in front of them.

Nevertheless, the bank in the second case was keen on improving its practices regarding the taping of telephone calls. In response, the Office developed a "best practices" guideline for recording customer telephone calls. Essentially, the guideline states that the taping of telephone calls involves the collection of personal information – a practice that should meet fair information principles. In other words, conversations should not be taped unless it is for a purpose that a reasonable person would consider appropriate in the circumstances. The customer must be informed of the purpose for taping the call and must consent, except in certain limited cases where consent is not required, before the taping begins. The customer should also be offered an alternative, such as not taping the call, visiting a retail outlet, writing a letter, or conducting the transaction over the Internet.

A tape recording captures more than just the specifics needed for the purpose of the call. It records comments, accents and attitudes – information that may not be relevant to the material required. For these reasons, it is important for organizations to be open with customers – to advise them that they record,

explain why they record, and offer them options if they do not want to be recorded.

In both complaints, we provided the banks with our “best practices” guideline and both organizations undertook improvements to their recording practices. In the first case, the bank now notifies customers at the beginning of a call that the conversation is being taped and provides them with alternative means of communicating their information should they not wish to proceed with the call. In the second case, the bank introduced a recorded message to inform all callers that conversations would be tape-recorded.

ISP holds e-mails “hostage”

A customer had complained when she learned that her Internet service provider (ISP) was continuing to receive and store her incoming e-mails while her account was suspended. This is in fact standard industry practice. Many ISPs use continued receipt and storage of e-mails as leverage in collecting on overdue payments.

In this case, the former Commissioner determined that the ISP had not properly informed the complainant of purposes related to the use of her personal information during an account suspension and had thus used her personal information without her informed consent for purposes other than those for which the information had been collected. On this basis, we concluded that the complaint was well-founded.

But this case left the Office highly concerned about the practice at issue, which we knew to be widespread in the industry. In the letters of findings, the former Commissioner commented as follows:

“... As Privacy Commissioner, I am concerned about the implications of storing and withholding potentially important messages without informing the intended recipient of their existence or the sender of their non-delivery. As an occasional sender of e-mails myself, rather than be falsely led to believe that a certain message had gone through unimpeded, I would much prefer to have it

returned with a notification of non-delivery so that I could try to reach the intended recipient by other means. Indeed, returning the message with a notification strikes me as the most appropriate and responsible course of action for an Internet service provider to take in such circumstances."

To answer the above question, then, what an ISP should do in cases of account suspension is what we recommended as best practices in the case in question, as follows:

- Cease collecting, storing, and denying access to, e-mails addressed to holders of accounts under suspension.
- Adopt instead the practice of deflecting such e-mails back to senders with notification to the effect that the messages could not be delivered.
- Make provision for giving the holder of a suspended account access to any e-mails already received by the company, but still unretrieved by the customer, at the time the suspension took effect.

Make sure to check those Government authorities

An individual's holiday memories were marred when he found out that the airline he had used for his trip released his itinerary to his boss. His employer, a federal Government department, was conducting an investigation into his use of sick leave. It approached the airline and requested confirmation of his travel itinerary.

The airline hesitated. Citing its responsibilities under the *PIPED Act*, it asked the department for proof that the individual had consented to such a disclosure. If that was not possible, the airline suggested that a specific exemption or exception under the *Act* would be needed before it would comply with the request.

In response, the department cited a directive under the authority of a specific federal statute, indicated that the information was needed to administer federal public servants' employment legislation, and asked the airline to disclose the itinerary. Satisfied that the department's request fit the exemption

provided in section 7(3)(c.1)(iii) of the *Act*, the airline duly released the information. This section allows an organization to release information about an individual to a Government institution for the purpose of administering a law.

There was just one problem. The department did not quote the correct directive as its lawful authority. Even though it later acknowledged its mistake, the department maintained that it nevertheless had the authority to collect the information – just under different legislation.

We agreed that the department had lawful authority. We were concerned, however, that the department had initially made an error and that the airline had not verified whether the cited directive was correct or not. Although the airline made the disclosure in good faith, an organization has a duty to be vigilant about checking authorities cited by Government organizations before releasing personal information. In his letter of findings the former Commissioner stated:

“...where requests for disclosure of personal information are concerned, I consider it incumbent upon any private-sector organization not to take the submissions of any government institution at face value, but rather to be vigilant about checking authorities cited.”

Fees for access: Should you have to pay for your own information?

Responding to requests for access to personal information may entail some costs for organizations. Should it also entail costs for the individual? In fact, there is a provision in the *Act* that allows organizations to charge a fee in responding to requests. But how much is reasonable? This question was addressed in two cases where the complainants accused organizations of charging excessively high fees.

The complainants were involved in disputes with their respective banks concerning money they had borrowed. Both individuals requested their personal

information. The banks responded by demanding fees of \$150 and \$200 respectively to cover the costs of processing the documents in question. The first individual wanted to know what he would get for his money and when told what this would be decided to file a complaint. The second individual is on a fixed income and could not afford to pay for his personal information.

These cases are good examples of the private sector adjusting to the expectations of the Act.

These cases are good examples of the private sector adjusting to the expectations of the *Act*. The banks were reminded that Principle 4.9.4 of the *PIPED Act* stipulates that an organization must respond to an individual's request at minimal or no cost to the individual. As a result, one bank released the information free of charge, while the other asked for a nominal fee of \$10.

Additionally, the bank's position in the first complaint seemed to be based not only on cost-recovery but also on its desire to have the complainant meet with it to discuss the dispute that had prompted the access request in the first place. We emphasized to the bank, however, that the *Act* does not require an individual to explain why he or she wants access to personal information or require that he or she enter into any discussions with an organization. In other words, personal information cannot be held for ransom.

Based on the findings in these cases, the bottom line for organizations when it comes to fees is this: cost-recovery does not apply to access to information requests.

A security clearance becomes a job requirement

Protecting nuclear sites from terrorist attacks is a grave concern, particularly in the wake of September 11, 2001. The federal agency that oversees the operations of all nuclear facilities in Canada responded to the terrorist threat by instructing its licencees to implement enhanced security measures. One of

the new measures in place is to limit entry to nuclear facilities to persons with the proper security clearance. If a licensee fails to comply, the federal agency will revoke its operating licence.

A company's nuclear products division informed its employees of the new security requirement and asked them to consent to a security clearance check. Along with a consent form, each employee received an information package that specified the type of information to be collected, the purpose, and the organization that would carry out the collection. Employees were also told that the organization collecting the personal information was bound by a confidentiality agreement.

In order to be granted a security clearance, employees with at least ten years of service were required to pass a criminal records check. Employees with less than ten years of service had to pass a full background check that included employment history, professional qualifications, and personal references, as well as a criminal records check.

Some employees were unhappy and complained to the Office. They felt they did not really have a choice – if they refused, they faced job loss. If they consented but failed the security check, they would lose their current positions and be reassigned, possibly to lower paying jobs. Under those circumstances, they felt their consent was coerced.

The former Commissioner had to determine whether the company was collecting personal information with the employees' knowledge and consent as required under Principle 4.3 of the *PIPED Act*. Clearly, the employees knew of the collection. But was their consent voluntary? In the letters of findings, the former Commissioner assessed the issue as follows:

"[The company] expressly asked you for your consent, and it is entirely up to you whether to give it or not. That there may be unpleasant consequences in either case does not alter the fact that you do have a choice in the matter. Refusal to give consent to the collection of personal information may very often entail unpleasant consequences for the individual. But in this case, as in most

decisions in life where the prospect of unpleasant consequences is a factor, the pressure you may feel to consent to the collection does not amount to duress. Under the Act, the key consideration is not whether there may be unpleasant consequences to an individual's refusal to give consent, but rather whether the collection is itself reasonable."

Was it reasonable for personal information to be collected for the purposes of a security clearance as stipulated by section 5(3) of the *Act*? The former Commissioner concluded that it is entirely reasonable for the federal agency to impose an enhanced security requirement upon its licencees, given the greatly enhanced concern about possible acts of terrorism at nuclear facilities. Had the company not complied, it would have lost its licence to produce nuclear fuels and would no longer have been able to conduct its nuclear products business, leading to substantial financial losses and staff lay-offs. Under these circumstances, we determined that it was entirely reasonable for the company to comply with the order and thus collect personal information from employees to conduct security clearance checks.

Aeroplan: Opt-out consent is not enough

When Air Canada mailed out privacy brochures to 60,000 Aeroplan members, several members complained to the Office.

The individuals who complained to the Office did not mind that the company had made the effort to seek their consent to information-sharing practices under the Aeroplan program. What they did object to, however, was having the onus put on *them* to tell Air Canada if they did *not* consent to the practices outlined in the brochure. Nor did they appreciate that the company was presuming, in the meantime, that they did consent.

The former Commissioner concluded that Air Canada was not in compliance with the *PIPED Act* and that the complaints were well-founded.

The 60,000 brochures accounted for only about one per cent of Aeroplan's total membership at the time. In the letters of findings, the former Commissioner

remarked that the *Act* required organizations to observe every individual's privacy rights and did not allow for token compliance. Since Air Canada had in effect left 99% of Aeroplan members in the dark about its information-handling policy and practices, the former Commissioner found its attempt at seeking consent to have been entirely inadequate.

Even if all plan members had been consulted, the brochure itself failed to seek consent in an appropriate form. It described five ways in which Air Canada was intending to share Aeroplan members' personal information under the program. Each description was accompanied by a check-off box, and the plan member was instructed to check the box only if he or she did not consent to having personal information shared in the manner described. Any plan member checking off one or more of the five boxes was then expected to mail the brochure back to the company by way of expressing non-consent. Conversely, any plan member who did not return the brochure was considered to have consented to all five information-sharing situations.

This form of consent has come to be known as "negative" or "opt-out" consent. It correlates to the "negative option" marketing practices that consumers have been so quick to condemn in the past. In effect, such practice is based on presumption – the individual is presumed to agree to a proposition unless he or she takes the initiative to refuse it.

Like most other people involved in the protection of privacy, and indeed like most informed consumers, we hold a very low opinion of the negative option as it is used

*Like most other people
involved in the
protection of privacy,
and indeed like most
informed consumers, we
hold a very low opinion
of the negative option as
it is used by
organizations in their
handling of personal
information.*

by organizations in their handling of personal information. The Office considers opt-out to be a weak form of consent – one that unfairly puts the onus of initiative on the wrong party and reflects at best a mere token observance of what is perhaps the most fundamental principle of the *Act*. We would prefer that organizations adopt an exclusively “positive” or “opt-in” approach – a much more respectful approach whereby individuals would be deemed to have consented only if they have expressed a definite “yes” to a proposition.

On the other hand, the Office is also well aware that opt-out is a form of consent expressly permitted by the *Act* in certain circumstances – notably, where the personal information is of a demonstrably non-sensitive nature. The problem here is that the *Act* itself refrains from precisely defining the notion of sensitivity. Although it does instruct that an individual’s financial and medical information is almost always to be considered sensitive, it also goes on to suggest that any information can be sensitive, depending on the context. In the Aeroplan complaints, therefore, the Office’s task was essentially one of assessing the context. In other words, the former Commissioner had to determine whether the circumstances justified Air Canada’s recourse to opt-out consent.

In the letters of findings, the former Commissioner made a point of stating that the intention is always to keep strict limits upon the circumstances in which opt-out could be deemed appropriate. It was also made clear that the Office intends to be guided in all such deliberations by due consideration for both the sensitivity of the information and the reasonable expectations of the individual. It was on these considerations that the Aeroplan privacy brochure ultimately failed.

The language of the brochure failed to demonstrate that any of the information-sharing situations described was strictly non-sensitive in nature or context. Two of the situations were of a particularly high order of sensitivity. The other three seemed by their descriptions to allow for considerable marketing to individuals on the basis of information customized according to potentially sensitive criteria. As it was put in the former Commissioner’s letters:

“Although in my view the practice of sharing plan members’ information for purposes of offering special promotions and products remains unobjectionable in itself, I am satisfied that a reasonable person would not expect such practice to extend to the ‘tailoring’ of information to the individual’s potentially sensitive interests, uses, and preferences without the positive consent of the individual.”

The former Commissioner concluded that it had been inappropriate for Air Canada to seek negative or opt-out consent to Aeroplan’s information-sharing policies and practices as described in the brochure.

To its credit, Air Canada took the Commission’s findings and recommendations very seriously. With some guidance from the Office, in a process that we found to be both positive and productive, the company undertook to rethink and rewrite its information-sharing policy under Aeroplan. We have reviewed the finished product, and have verified that the policy now addresses our concerns in the following ways:

- It explains to Aeroplan members, in clear and understandable terms, the purposes for the collection, use, and disclosure of personal information under the program.
- It explains clearly that Aeroplan does not collect any details of the transactions whereby members accumulate points under the program.
- It specifies that Aeroplan does not provide individualized profiles of members to partner companies or other third parties, and further clarifies that any information provided to partners can be used only for purposes related to the Aeroplan program.
- It explicitly and clearly states that members who wish to have their personal information used only for redemption of Aeroplan points can so stipulate, and it identifies an easily-executable procedure for members to exercise this option.

As for the matter of consulting the full Aeroplan membership, Air Canada also set out a very specific plan whereby all active members of the program would

receive a copy of the revised policy with their next account statements. Moreover, the policy was to be made available on the Aeroplan Web site.

We were satisfied that Air Canada had responded appropriately to our recommendations, and pleased with the spirit of co-operation the company has shown.

A case of deception

It is one thing to do a poor job of informing individuals of the purposes for which their information would be used, as three of the above-mentioned organizations did. It is quite another to deliberately misinform, as we found to be the case in a complaint against a market research firm.

This firm mails questionnaires for what it calls “consumer product surveys” to households across Canada. The questionnaires ask about household preferences among various categories of products. The literature accompanying each questionnaire explains the purpose of the survey strictly in terms of “fact-finding,” seeking householders’ “opinion” and understanding consumer “preferences and attitudes,” all with a stated view to improving the quality, life and value of products.

However, the surveys were truly intended for the purpose of selling products to the survey respondents. What the survey firm mainly intends to do with the personal information it collects in the questionnaires is compile customized mailing lists, which it will then give to the third-party companies that have commissioned the given survey. These commissioning companies will then attempt to sell products to the survey respondents by directly marketing them according to the information they have provided in the questionnaires.

The *PIPED Act* says that an organization has to identify its true purposes for collecting personal information. It also says that consent to the collection of personal information must not be obtained through deception.

If an organization intends to give information it collects to direct marketers, it has to say so, in no uncertain terms and in a manner that people can reasonably understand. In the survey literature in question, there is neither an explicit statement nor even a reasonably understandable implication to the effect that personal information of individual respondents will be disclosed to third parties.

*If an organization
intends to give
information it collects
to direct marketers,
it has to say so...*

The questionnaire does ask for the respondent's consent to further mailings and offers, but says nothing about where such communications would come from. In the absence of any indication that the survey firm intends to share the respondent's mailing address with other possible mailers, the most reasonable inference would be that any further mailings would come from the same source as the original – that is, from the survey firm itself.

Furthermore, the consent mechanism is a problem in itself. Given that many of the survey questions are highly sensitive in nature (notably, several have to do with personal health and finances), the “opt-in” form of consent should be used in the circumstances. But the consent mechanism has two check-off boxes, one for “yes” and the other for “no”, and is thus ambiguous as to the form of consent intended. What happens in fact, however, in the not-infrequent cases where the respondent checks off neither box, is that the individual is presumed to give consent to further mailings. Thus, the survey firm is using the “opt-out” form of consent in a situation that clearly calls for “opt-in.”

The survey literature also does mention that companies have commissioned the survey. However, it does not name the commissioning companies. Nor does it in any discernible way suggest that these anonymous companies are direct marketers, or that what they have in effect commissioned from the survey firm is the collection of prospective customers' personal information on

their behalf. Indeed, there is nothing in the literature that gives the individual householder any substantial grounds to believe that the survey is anything other than what it purports up front to be – that is, strictly a fact-finding, opinion-seeking market study aimed at product improvement.

On the basis of such a description, respondents might reasonably expect that the survey's sponsors would receive results in the form of aggregated, anonymized analytical data. But respondents are given no legitimate reason to expect, and every good reason to resent, that as a result of their participation in the survey they may soon be subject to intrusive and unwanted direct-marketing efforts by third-parties who have been made privy to their sensitive personal information.

It may seem paradoxical to some that, despite the overwhelming case against the survey firm on these and other counts, what troubled us most was evidence of the firm's *compliance* with the *Act*.

The firm does, in fact, have an official written privacy policy pertaining to its household surveys posted on its Web site. This policy does a relatively good job of identifying the true purposes for collecting the survey information. However, not only is this policy not included or otherwise reflected in the survey literature mailed to households, but it is not made reasonably accessible to householders. The survey literature does not even mention the existence of the Web site, let alone that of the policy.

What troubled us specifically were the implications of the vast discrepancy in compliance between the Web site and the survey literature. In the letters of findings, the former Commissioner raised the concerns as follows:

“Why would [the firm] make reasonably clear in a remote and unadvertised privacy policy, but not at all clear in survey materials actually provided to individuals, that respondents’ personal information would be disclosed to third parties for marketing purposes? Why in the survey materials would [the firm] explain the purposes of its surveys only in such limited terms as fact-finding, opinion-gathering, and product quality improvement, and relegate to a document that

no one would ordinarily ever see the further purpose of direct marketing by third parties? Indeed, why would [the firm] take pains to formulate a more or less compliant privacy policy and then not draw attention to that policy when it truly mattered, in effect hiding the policy from customers?

"In brief, I find it difficult to comprehend this discrepancy, except in terms of deception. [The firm] has suggested that its survey materials serve to produce a reasonable expectation of disclosure to, and direct-marketing by, third parties. I cannot see, however, that any previously unsuspecting person could reasonably infer such a purpose from the scant, vague, and misleading indications provided. Rather, in my considered view, far from being conducive to a reasonable understanding of how personal information will be used or disclosed, the survey materials serve only to deceive individuals as to the true purposes of the surveys and to detract from the fairness of [the firm's] collection of personal information."

An advocacy group's expectations about consent

The *PIPED Act* states, at Principle 4.3.5 of Schedule 1, that the reasonable expectations of the individual are relevant in matters of consent. But it does not elaborate.

Rather, it leaves us the difficult task of interpreting this provision. In the circumstances of any consent-related complaint, it is often up to the Commissioner to determine the reasonableness of a complainant's expectations and the extent of their relevance. Fortunately, fairly early in the life of the *Act*, a body of complaints arose that we found useful in formulating a general position on what an individual may reasonably expect in matters of consent.

An individual filed complaints on behalf of an advocacy group against two banks, a telecommunications company, and a company that ran a frequent-buyer program. All the complaints were basically the same – that the organizations in question were not obtaining valid informed consent from individuals to disclosures of their personal information for marketing purposes.

The complaints consisted of two main allegations. The first was that the organizations were not making reasonable efforts to inform clients that their personal information was to be disclosed to third parties for secondary marketing purposes – that is, purposes additional to those for which the information needed to be collect-

ed in the first place. The complainant's contention was that, if individuals were not being properly informed of secondary purposes, the organizations had no valid basis for presuming the individual's consent to such purposes. The second main allegation was that, despite their reliance on the "opt-out" form of consent, the organizations were not providing reasonable opportunities for individuals to opt out of third-party marketing.

*To us, these
assumptions clearly
represented
"expectations" on the
complainant's part.*

As interesting as the allegations themselves were their underlying assumptions, which the advocacy group had presented in a position statement supporting the complaints. To us, these assumptions clearly represented "expectations" on the complainant's part. Before determining whether or not the organizations in question were in compliance with the relevant consent provisions of the *Act*, we thought it prudent to consider whether the group's expectations regarding consent were themselves reasonable in relation to the *Act*.

After analyzing them, the former Commissioner concluded that the group's expectations were entirely reasonable. Notably, the former Commissioner found it reasonable to expect the following from organizations that use or disclose personal information for secondary purposes:

- It is not enough to identify purposes in privacy policy documents and make such documents generally available. An organization should bring its secondary purposes directly to the attention of the individual at the time of

collecting personal information. During an application or a subscription process, for example, the individual should be presented with the necessary information and should not be referred to sources not immediately at hand. (These expectations are supported by Principles 4.2.3 and 4.3.1 of the *Act*, which instruct that identification of purposes and seeking of consent be direct and coincident with the collection of personal information.)

- Purposes should be stated in clear, plain language understandable to the ordinary consumer and in adequate detail for the consumer to appreciate the nature and extent of the intended collections, uses, and disclosures. (These expectations are supported by Principle 4.3.2, which instructs that purposes be stated in such a manner that the individual can reasonably understand how personal information will be used or disclosed.)
- If purposes are identified in writing, the individual should not be required to read fine print in dense passages.

Where an organization intends to presume the individual's consent to secondary purposes, the organization should provide a convenient opportunity for the individual to opt out. The opportunity and the procedure for opting-out should likewise be brought to the individual's attention at the time of collecting the personal information. The opting-out procedure should be easy, immediate, and inexpensive.

On this basis, and upon investigation of the actual policies and practices of the organizations, the Commissioner concluded that two of the complaints were well-founded and two were not. The former Commissioner found that the telecommunications company was not making any disclosures of the kind alleged, since it was prohibited from doing so by the CRTC. One bank was indeed disclosing personal information for secondary marketing purposes as alleged, but the former Commissioner found it to be making reasonable efforts on the whole to inform account applicants of the practice, obtain their consent to it, and provide them with an opt-out opportunity.

In the well-founded cases, the non-compliance of the frequent-buyer program was largely a matter of inconsistency in enrolment procedures. The case of the second bank, however, was much more serious. This bank's efforts at obtaining informed consent from account applicants did not in any respect meet the requirements of the *Act* or the reasonable expectations of the individual. In the letter of findings, the former Commissioner commented on the various materials used by the bank to communicate purposes, and on the nature and extent of the failed compliance in this case:

"The wording ... is so broad in each case as to virtually preclude understanding, unless the individual is to understand that the bank intends to use personal information however it may see fit and disclose it to whomever it may see fit. This would hardly be a purpose that any reasonable person would expect or consider appropriate in any circumstances."

By positive contrast, it should be noted that, in the case of the first bank, the former Commissioner complimented the bank on its approach to obtaining informed consent from account applicants. For those applying in person at branches, this bank's application procedure involved sitting the individuals down, providing them with the appropriate privacy information on the spot, drawing their attention specifically to statements of secondary marketing purposes, asking whether they consented or not to specific marketing practices, and recording and abiding by their responses. We regard such procedure as exemplary, amounting to the positive form of consent that we prefer.

Consent to secondary purposes

What follows is a summary of the deliberations to date in cases relating to consent to secondary purposes.

- Positive or opt-in consent is always to be preferred as the form of consent that is strongest, most respectful of individuals, and best in keeping with the spirit of the *Act*. Organizations are encouraged to adopt this form of consent exclusively.

- Positive or opt-in consent to secondary purposes is a requirement in situations where the personal information is sensitive in itself or where there is a significant potential for the information to be rendered sensitive in the context of the information-handling activities.
- Since the *Act* indicates that personal information of a financial or medical nature is almost always to be considered sensitive, these types of information will almost always be deemed to warrant positive consent. However, since the *Act* also stipulates that any personal information may be sensitive in a given context, no further attempt should be made to precisely define the notion of sensitivity. Rather, the context should be considered in each case, with a view to determining the potential for sensitivity.
- Two prime considerations in determining the potential for sensitivity of personal information are the intent to disclose the information to third parties and the intent to categorize or otherwise process the information according to personal criteria.
- Negative or opt-out consent, also known as presumed consent, despite being the weaker and less preferable form, is recognized under the *Act* as being acceptable in certain circumstances. The scope of circumstances in which this form of consent is allowable will remain limited.
- An organization's use of the negative or opt-out form of consent to secondary purposes will be deemed justified only under the following conditions:
 - The personal information must be of a demonstrably non-sensitive nature and context and must be identified by item or type.
 - If the information is to be disclosed to third parties, the parties must be identified by name or type.
 - The organization must state its purposes in full accordance with Principles 4.2, 4.2.3, 4.3.1, and 4.3.2 and with the individual's reasonable expectations as deemed relevant in Principle 4.3.5. Specifically, the identified purposes must be brought directly to the individual's attention, either orally or in writing, at the time the personal information is collected (e.g., during the subscription, application, or enrolment process); in clear, specific, unambiguous terms; in a format easy to read (where text is used); and in a manner conducive to the

individual's understanding of how exactly the personal information is to be used or disclosed.

- The organization must provide an appropriate "opt-out" mechanism – that is, a convenient opportunity and procedure for withdrawal of consent. The mechanism must be brought to the individual's attention at the time the personal information is collected and should be inexpensive, easy to execute, and immediately effective in withdrawing consent. Where feasible, it should include a toll-free number.

INCIDENTS UNDER THE *PIPED ACT*

Checking up on telephone calls

A journalist contacted the Office about a survey being conducted on behalf of a telephone company by a research firm. It appeared as though the company was gathering information from customers about their telephone calls.

The research firm had a contract with the telephone company to carry out random checks for quality assurance purposes. The telephone company provided the firm with the phone number of customers who had made calls seeking assistance by dialing "0" or "411." The firm was not given the names of the customers or other identifying information. The company has a non-disclosure contract with the research firm, which requires the firm to destroy the information it collects once the results of the survey are compiled.

The former Commissioner was satisfied when it was determined that the telephone company was complying with a CRTC requirement to conduct regular quality of service measurements of the accuracy of Directory Assistance services.

Dumpster find

A bank alerted the Office that confidential client documents had been found in a dumpster located near a branch that had closed some time earlier. The building had been leased to a new tenant and was being renovated. Apparently the renovators found the documents during the reconstruction and disposed of them. Upon hearing of the matter, the media retrieved some of the documents from the dumpster.

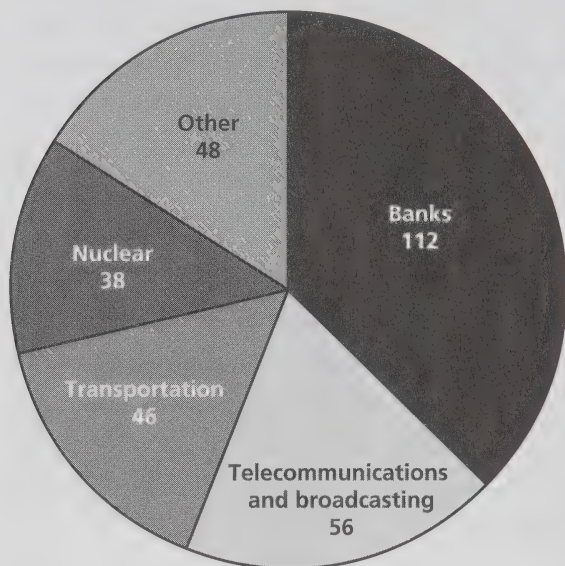
The bank took prompt action as soon as it became aware of the situation by recovering all of the documents from the dumpster and the journalists; then it verified that no other bank documents remained in the building. The bank also informed each of the affected customers, either in person or in writing, of the incident and of the steps it had taken to recover the documents. In addition, the bank apologized to each customer and assured each one that all of their information had been recovered.

It was determined that the branch in question was amalgamated with another, and a private company on contract to the bank was tasked with sorting through and processing records. The bank has established procedures for this, but the private company did not follow these properly, with the result that some documentation was not appropriately classified and was disposed of incorrectly. The bank subsequently clarified procedures with the private company.

The former Commissioner was satisfied that the bank acted promptly and appropriately in dealing with this sensitive situation.

Complaints Received by Sector

January 1, 2002 to December 31, 2002



Inquiries under the *PIPED Act*

January 1, 2002 to December 31, 2002: 8,381

We will attempt to provide a breakdown of these inquiries by subject in future Annual Reports.

PRIVACY PRACTICES AND REVIEWS

The *Personal Information Protection and Electronic Documents (PIPED) Act* enables the Commissioner to audit the compliance of private sector organizations if there are reasonable grounds to believe that they are in contravention of the *Act* or are not following a recommendation set out in Schedule 1 (ten principles). The Privacy Practices and Reviews (PP&R) Branch will conduct such compliance reviews and audits under section 18 of the *PIPED Act*, following accepted standard audit objectives and criteria. During the period under review, there were a number of issues that were brought to the Commission's attention that were successfully resolved without the necessity of conducting an audit. For example, Office of the Privacy Commissioner staff met and advised representatives of an industry association on the viability of obtaining direct consent and the proposed contents of such a consent form. We provided guidance to a business with respect to the use of the SIN as an identifier and the use of opt-out consent. As well, we provided a comprehensive review and analysis of a corporate privacy policy.

Apart from those issues, the former Commissioner was not aware of any other concerns that would provide sufficient grounds to initiate an audit under the law.

Nevertheless, the PP&R Branch has been involved in consulting with and providing advice to private sector organizations that come under the jurisdiction of the *PIPED Act*. It has also assisted those organizations that are not currently governed by the *Act* but that are preparing for January 1, 2004, when the *Act* will begin to apply to them.

IN THE COURTS

Under section 14 of the *Personal Information Protection and Electronic Documents (PIPED) Act*, an individual complainant has a right, following the Commissioner's investigation, to apply to the Federal Court of Canada for a hearing in respect of any matter that is referred to in the Commissioner's report. These matters must be among those in the listed Schedule clauses and sections of the *PIPED Act*.

Section 15 of the *Act* allows the Commissioner to apply to appear in Federal Court. The Commissioner may, with the consent of the complainant, apply directly to the court for a hearing in respect of any matter covered by section 14; appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or, with the leave of the Court, appear as a party to any section 14 hearing.

Following is a list of all *PIPED Act* applications in the courts from January 1, 2001 to December 31, 2002:

Mathew Englander v. Telus Communications Inc.

Federal Court File No. T-1717-01

This is the first application for judicial review to be filed in the Federal Court under the *PIPED Act*. Mr. Englander argues that Telus uses and discloses customers' names, addresses and telephone numbers in its white pages directories and otherwise, without customers' knowledge and consent, and inappropriately charges customers for choosing to have their telephone number "non-published." He claims that these actions by Telus contravene subsections 5(1) and (3) of the *PIPED Act*, as well as several clauses of Schedule 1 of the *PIPED Act*.

Status

This Application was dismissed on June 2, 2003.

Ronald G. Maheu v. the Attorney General of Canada and IMS Health Canada

Federal Court File No. T-1967-01

Ronald Maheu applied for a hearing in the Federal Court arguing that IMS Health Canada improperly discloses personal information by selling data on physicians' prescribing patterns without their consent.

Status

Mr. Maheu filed an Amended Notice of Application in March 2002. IMS brought a motion seeking either to strike out the Application on the grounds that it was brought for an improper purpose or to have Mr. Maheu post security for costs. The Court ordered Mr. Maheu to post security for costs in the amount of \$12,000 and noted that there appeared to be reason to believe that Maheu was using the *Act* for a collateral and improper purpose given that his own personal information was not at issue. On appeal, the former Commissioner appeared to assist the Court with respect to the proper interpretation of the *PIPED Act*, explaining that an individual may file a complaint concerning an organization's information practices regardless of whether that organization collects, uses or discloses personal information about the individual complainant. The Federal Court agreed with this position and granted Mr. Maheu's appeal on January 3, 2003. This decision is currently being appealed, and the original Application continues to proceed in Trial Division.

Diane L'Ecuyer v. Aéroports de Montréal

Federal Court File No. T-2228-01

Diane L'Ecuyer complained that Aéroports de Montréal had sent copies of a letter of response to access requests she had made to two union representatives and an employee relations co-ordinator and had, therefore, disclosed personal information without her consent. The former Commissioner investigated her complaint and, among the findings, recommended that individuals must be allowed to judge for themselves whether or not to share such a response with others.

Status

Madame L'Ecuyer applied to Federal Court on December 18, 2001, seeking an Order that the organization correct its practices to conform with the *PIPED Act* and that the organization publish a notice stating any action taken or proposed to be taken to correct its practices. On May 13, 2003 the Trial Division released its decision, finding that the issue arose from the administration of a collective agreement and therefore was not within the jurisdiction of the Privacy Commissioner. Madame L'Ecuyer filed an appeal of that decision on June 5, 2003 and the Privacy Commissioner is preparing to apply for leave to intervene in that appeal.

Nancy Carter v. Inter.net Canada Limited

Federal Court File No. T-1745-02

Nancy Carter contacted the Office with concerns about the practice(s) of her Internet Service Provider (ISP). During a billing dispute with the complainant, the ISP had suspended her access to e-mail, but continued to keep the account active and accepted new e-mails into the mailbox. The claimant argues that she was therefore denied access to her personal information contrary to the *PIPED Act*, and lost a valuable business opportunity as a result. She is seeking damages under the *PIPED Act*.

Status

A settlement was reached in this case and accordingly a Notice of Discontinuance was filed on June 5, 2003.

Sylvain Gagné v. Bell Canada

Federal Court File No. T-1971-02

Sylvain Gagné complained to the Office that (a) that he had been denied access to some of his personal information and (b) of the improper disclosure of the personal information of others. Although the former Commissioner found the denial of access complaint to be not well-founded, agreeing that exemptions under 7(1)(b) and 9(3)(c.1) had been correctly applied, the complaint about the disclosure of personal information was well-founded and the former Commissioner issued recommendations as to change of practices.

Status

The Notice of Application was filed in Federal Court on November 25, 2002, requesting a variety of relief, including access to the withheld documents, damages to those affected, and Orders enforcing the Office's recommendations.

Bell Canada has now agreed to follow the Office's recommendations, and thus a Notice of Discontinuance was filed on March 14, 2003.

Dale Stuart v. the Toronto Dominion Bank

Federal Court File No. T-290-02

Dale Stuart believed that information about his banking affairs had been disclosed by employees of the TD Bank to his employer without Mr. Stuart's knowledge or consent.

Status

This application was discontinued by Mr. Stuart on December 2, 2002.

Yukon Hospital Corporation v. Attorney General of Canada

Federal Court File No. T-1814-02

This action was initiated in response to the former Commissioner's determination that he had jurisdiction under section 4(1)(b) to conduct an investigation of a complaint filed against the Yukon Hospital Corporation.

Status

A complaint was filed with this Office under the *Privacy Act*. Although the Yukon Hospital Corporation is governed by the *PIPED Act*, the complaint was originally made under the *Privacy Act*. After discussions with the Applicant to this effect, the former Commissioner withdrew his decision to investigate the complaint. Court proceedings were discontinued on February 21, 2003.

Keith Vanderbeke v. Royal Bank of Canada

Federal Court File No. T-2185-02

Keith Vanderbeke contacted the Office complaining that the Royal Bank of Canada had denied him access to three documents pertaining to a commercial mortgage for which he personally was the guarantor.

Status

In the application, the claimant is specifically seeking (among other things) interpretive Orders relating to the *PIPED Act*: an Order that a private corporation may be an “identifiable individual” under the *PIPED Act* with attendant access rights; and an Order that private corporation banking documents should be considered personal documents where a natural person has provided a personal guarantee to the creditor. It is uncertain whether this aspect will be allowed to continue because, among other things, the part of the Application apparently brought pursuant to section 14 of the *PIPED Act* improperly seeks review of the former Commissioner’s findings. Under section 14 of the *PIPED Act*, the only proper respondent is the Royal Bank of Canada.

Part Three

Corporate Services

On April 1, 2002, the Office of the Privacy Commissioner of Canada ceased to share corporate services with the Office of the Information Commissioner of Canada, and established its own Corporate Services Branch.

The Corporate Services Branch provides advice and services in the areas of finance, human resources, information technology and administration to the Office's senior managers and staff.

As noted in the Foreword, the House of Commons Committee on Government Operations and Estimates has, in the course of examining the operations of the Office, uncovered a number of serious problems related to some of these areas. As well, the Office is the subject of reviews by both the Office of the Auditor General of Canada and the Public Service Commission of Canada.

I intend to use the results of these reviews to ensure that the Office is managed in a manner that is accountable to Parliament and respects the policies and regulations applicable to the public service.

At the beginning of fiscal year 2002-2003, the Office's budget was \$11.1 million, the same as our budget for the previous year. During the course of the year,

our budget was adjusted upward by \$773,000, primarily to offset increased legal costs, costs associated with the Government's new Privacy Impact Assessment Policy and collective bargaining salary increases, for a total budget of \$11.9 million.

Our expenditures totalled \$12.2 million. We exceeded our budget by \$240,000 largely due to changes in accounting practices in order to be consistent with the principles of accrual accounting in the federal government.

The Office is currently reviewing its financial resources, in conjunction with the Treasury Board Secretariat, to ensure that it has the resources needed to fulfill its obligations in fiscal year 2003-2004 and beyond in anticipation of the full and final implementation of the *PIPED Act* on January 1, 2004.

Resources

April 1, 2002 to March 31, 2003

	Expenditure Totals (\$)	% of Totals
Privacy Act	5,208,588	43%
PIPED Act	5,582,722	46%
Corporate Services	1,367,778	11%
Total	12,159,088	100%

Note that as of March 2003 there were 103 full-time staff at the Office of the Privacy Commissioner of Canada.

Detailed Expenditures¹*April 1, 2002 to March 31, 2003*

	Privacy Act	PIPED Act	Corporate Services²	Total
Salaries	3,462,955	2,845,391	808,513	7,116,859
Employee Benefits Program	657,386	595,000	240,220	1,492,606
Transportation and Communication	284,228	352,412	67,005	703,645
Information	25,649	315,406	34,592	375,647
Professional Services	679,897	700,870	65,526	1,446,293
Rentals	12,840	2,202	11,648	26,690
Repairs and Maintenance	8,607	41,249	5,447	55,303
Materials and Supplies	44,328	5,012	51,699	101,039
Acquisition of Machinery and Equipment	29,100	725,180	83,128	837,408
Other Subsidies and Payments	3,598	-	-	3,598
Total	\$5,208,588	\$5,582,722	\$1,367,778	\$12,159,088

Notes:

¹ Total expenditure figures are consistent with public accounts.

² Effective April 1, 2002, Corporate Services is part of this Office and resources are no longer shared with the Office of the Information Commissioner of Canada.

Dépenses détaillées¹

1^{er} avril 2002 – 31 mars 2003

Loi sur la protection des renseigne- ments personnels et les documents électroni- ques	Loi sur la protection des renseigne- ments personnels	Services de gestion ²	Total	Salaires et traitements	Cotisations au régime d'avantages sociaux des employés	Transports et communications	Information	Services professionnels	Locations	Réparations et entretien	Approvisionnements et fournitures	Achat de machines et d'équipements	Autres subventions et paiements	Total
				3 462 955	657 386	284 228	25 649	679 897	12 840	8 607	44 328	29 100	3 598	5 208 588 \$
				2 845 391	595 000	352 412	315 406	700 870	2 202	41 249	5 012	725 180	-	5 582 722 \$
				808 513	240 220	67 005	34 592	65 526	11 648	5 447	51 699	83 128	-	1 367 778 \$
				7 116 859	1 492 606	703 645	375 647	1 446 293	26 690	55 303	101 039	837 408	3 598	12 159 088 \$

Nota :

¹ Les dépenses totales correspondent aux comptes publics.

² À compter du 1^{er} avril 2002, les Services de gestion font partie du Commissariat et leurs services ne sont plus partagés avec le Commissariat à l'information du Canada.

Au début de l'année fiscale 2002-2003, le budget du Commissariat était de 11,1 millions de dollars, le même que notre budget pour l'année précédente. Au cours de l'année, notre budget a connu un ajustement à la hausse de 773 000 \$, principalement pour faire face à une augmentation de coûts juridiques associés avec la nouvelle politique de l'Analyse des facteurs relatifs à la vie privée fédérale, et aux augmentations reliées à la négociation collective, pour un budget total de 11,9 millions de dollars.

Nos dépenses ont totalisé 12,2 millions de dollars. Nous avons excédé la limite de notre budget de 240 000 \$, en grande partie à cause des pratiques de la comptabilité d'exercice afin d'être conforme aux principes de comptabilité d'exercice du gouvernement fédéral.

Le Commissariat révisé actuellement ses ressources financières, conjointement avec le Secrétaire du Conseil du Trésor, afin de s'assurer qu'il a des ressources dont il a besoin pour s'acquitter de ses obligations en vue de l'année 2003-2004, et au-delà en prévision de la mise en œuvre complète et finale de la LPRPD le 1^{er} janvier 2004.

Resources

1^{er} avril 2002 – 31 mars 2003

Dépenses globales (\$)		Pourcentage du total
Loi sur la protection des renseignements personnels		43 %
Loi sur la protection des renseignements personnels et les documents électroniques		46 %
Services de gestion		11 %
Total		100 %

À noter que depuis mars 2003, il y a eu 103 employées à temps plein au Commissariat à la protection de la vie privée du Canada.

Partie III

Services de gestion

Le 1^{er} avril 2002, le Commissariat à la protection de la vie privée du Canada a cessé de partager les services de gestion avec le Commissariat à l'information du Canada, et a créé sa propre Direction de la gestion intégrée.

La Direction de la gestion intégrée fournit à la fois des conseils et des services de gestion intégrée dans les domaines de la finance, des ressources humaines, de la technologie de l'information et des services administratifs aux cadres supérieurs et au personnel du Commissariat.

Tel qu'il est mentionné dans la préface, le Comité des opérations gouvernementales et des prévisions budgétaires a relevé un certain nombre de problèmes sérieux liés à certains de ces secteurs, au cours de son enquête relativement aux opérations du Commissariat. En outre, le Commissariat a fait l'objet d'examen menés à la fois par le Bureau de la vérificatrice générale du Canada et la Commission de la fonction publique du Canada.

J'ai l'intention d'utiliser les résultats de ces examens pour m'assurer que le Commissariat est géré de façon à être imputable au Parlement, et observe les politiques et les règlements applicables au secteur public.

Société de l'hôpital du Yukon c. Solliciteur général du Canada

N° de dossier de la Cour fédérale du Canada : T-1814-02

Ce recours a été introduit en réponse à la détermination par l'ancien commissaire selon laquelle il avait compétence en vertu de l'alinéa 4(1)b) de faire enquête sur une plainte déposée à l'encontre de la Société de l'hôpital du Yukon.

État de la situation

Une plainte a été déposée au Commissariat en vertu de la Loi sur la protection des renseignements personnels. Bien que la Société de l'hôpital du Yukon soit régie par la LPRPDE, la plainte a été initialement déposée en vertu de la Loi sur la protection des renseignements personnels. Après discussion avec le requérant à cet effet, l'ancien commissaire est revenu sur sa décision de faire enquête sur la plainte. Les procédures légales ont été abandonnées le 21 février 2003.

Keith Vanderbeke c. Banque Royale du Canada

N° de dossier de la Cour fédérale du Canada : T-2185-02

Keith Vanderbeke a communiqué avec le Commissariat se plaignant que la Banque royale du Canada lui avait refusé l'accès à trois documents relatifs à une hypothèque commerciale pour laquelle il était personnellement le garant.

État de la situation

Dans la demande, le plaignant recherche particulièrement, entre autres choses, des ordonnances interprétatives relatives à la LPRPDE : une ordonnance selon laquelle une entreprise privée pourrait être une « personne identifiable » en vertu de la LPRPDE, jouissant corrélativement de droits d'accès ; et une ordonnance selon laquelle les documents bancaires de l'entreprise privée devraient être considérés comme des documents personnels lorsqu'une personne physique fournit une garantie personnelle au créancier. Il n'est pas sûr que le traitement de cet aspect soit poursuivi car, entre autres, la partie de la demande apparemment présentée en vertu du paragraphe 14 de la LPRPDE vise à faire réviser de façon inappropriée les conclusions de l'ancien commissaire. Le seul défendeur légitime, en vertu du paragraphe 14 de la LPRPDE, est la Banque royale du Canada.

Sylvain Gagné c. Bell Canada

N° de dossier de la Cour fédérale du Canada : T-1971-02

Sylvain Gagné s'est plaint au Commissariat (a) du fait qu'on lui avait refusé l'accès à certains de ses renseignements personnels et (b) d'une communication inappropriée de renseignements personnels concernant d'autres personnes. Même si l'ancien commissaire a conclu que la plainte de refus d'accès était non fondée, en acceptant le fait que les exemptions en vertu de 7(1)(b) et 9(3)(c.1) avaient été correctement appliquées, la plainte sur la communication de renseignements personnels était fondée et l'ancien commissaire a formulé des recommandations concernant les changements à apporter aux pratiques.

État de la situation

L'avis de demande a été présenté à la Cour fédérale le 25 novembre 2002, demandant une série de dispenses, dont l'accès aux documents qui n'ont pas été communiqués, des dédommagements pour les personnes touchées et des ordonnances donnant pouvoir exécutif aux recommandations.

Bell Canada a maintenant accepté de suivre les recommandations du Commissariat et un avis d'abandon a alors été déposé le 14 mars 2003.

Dale Stuart c. la banque Toronto Dominion

N° de dossier de la Cour fédérale du Canada : T-290-02

Dale Stuart croyait que des renseignements relatifs à ses affaires bancaires avaient été communiqués par des employés la banque TD à son employeur à son insu et sans son consentement.

État de la situation

Cette demande a été abandonnée par M. Stuart le 2 décembre 2002.

commissaire a fait enquête sur sa plainte et recommandé dans ses conclusions que les personnes devraient être en mesure de juger par elles-mêmes si elles désiraient ou non partager une telle réponse avec les autres.

État de la situation

Madame L'Écuyer a fait une demande à la Cour fédérale le 18 décembre 2001, demandant qu'une ordonnance soit formulée exigeant que l'organisation corrige ses pratiques pour se conformer à la *LPRPDE* et que l'organisation publie un avis mentionnant toutes les mesures prises ou proposées afin de corriger ses pratiques. La Section de première instance a rendu sa décision le 13 mai 2002 et conclu que la question s'est posée dans le cadre de l'administration d'une convention collective et que, par conséquent, le commissaire à la protection de la vie privée n'avait pas compétence dans cette cause. Madame L'Écuyer a fait appel de la décision le 5 juin 2003 et le commissaire à la protection de la vie privée envisage demander une autorisation pour intervenir dans cet appel.

Nancy Carter c. Internet Canada Limited

N° de dossier de la Cour fédérale du Canada : T-1745-02

Nancy Carter a fait part de ces préoccupations au Commissariat concernant les pratiques d'un fournisseur d'accès Internet (FAI). Au cours d'une dispute concernant la facturation avec la plaignante, le FAI avait suspendu son accès à sa boîte de courrier électronique, mais le compte était toujours actif et acceptait les nouveaux messages électroniques dans la boîte aux lettres. La plaignante affirme qu'elle était ainsi donc privée d'accès à ses renseignements personnels, ce qui va à l'encontre de la *LPRPDE* et qu'elle a perdu des possibilités d'affaires précieuses à la suite de cet incident. Elle réclame donc un dédommagement en vertu de la *LPRPDE*.

État de la situation

Une entente a été conclue dans cette affaire et un avis d'abandon a été déposé le 5 juin 2003.

Ronald G. Mahou c. le procureur général du Canada et IMS Health Canada

N° de dossier de la Cour fédérale du Canada : T-1967-01

Ronald Mahou a demandé une audience à la Cour fédérale du Canada, soutenant qu'IMS Health Canada avait communiqué de manière inappropriée des renseignements personnels en vendant des données sur les habitudes de prescription des médecins sans avoir obtenu leur consentement.

État de la situation

M. Mahou a déposé un avis de demande modifié en mars 2002. IMS a présenté une requête demandant de soit rejeter la demande sur des motifs voulant que la demande ait été présentée à des fins inappropriées ou soit de demander à M. Mahou de verser une garantie pour les coûts. La Cour a ordonné à M. Mahou de déposer une garantie financière de 12 000 \$ et a mentionné qu'elle avait des raisons de croire que M. Mahou utilisait la Loi à des fins accessoires et inappropriées, compte tenu du fait que ses propres renseignements personnels n'étaient pas en jeu. Lors de l'appel, l'ancien commissaire a comparu pour apporter son aide à la Cour relativement à l'interprétation adéquate de la LPRPD, expliquant qu'une personne peut déposer une plainte concernant les pratiques de renseignements personnels d'une organisation sans égard au fait que celle-ci recueille, utilise ou communique des renseignements personnels la concernant. La Cour fédérale a accepté cette position et a accordé un appel à M. Mahou le 3 janvier 2003. Cette décision est actuellement en appel et la demande originale est encore traitée à la Section de première instance.

Diane L'Ecuier c. Aéroports de Montréal

N° de dossier de la Cour fédérale du Canada : T-2228-01

Diane L'Ecuier s'est plainte que les Aéroports de Montréal avaient envoyé des copies d'une lettre de réponse aux demandes d'accès qu'elle avait faites à deux représentants du syndicat et à un employé du coordinateur des relations et qu'ils avaient, par conséquent, communiqué des renseignements personnels à son sujet sans avoir obtenu son consentement. L'ancien

DEVANT LES TRIBUNAUX

Aux termes de l'article 14 de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), une personne ayant porté plainte a le droit, à l'issue de l'enquête du commissaire, de déposer une demande d'audience à la Cour fédérale du Canada sur toute question dont il est fait mention dans le rapport du commissaire. Ces questions doivent figurer parmi les clauses énoncées dans l'annexe, ainsi que dans les articles de la LPRPDE.

Aux termes de l'article 15 de la LPRPDE, le commissaire est autorisé à déposer une demande de comparution à la Cour fédérale. Il peut, avec le consentement du plaignant, demander directement une audience à la Cour sur toute question visée à l'article 14 ; comparative devant la Cour au nom de tout plaignant qui a présenté une demande d'audience en vertu de l'article 14 ; ou, avec l'autorisation de la Cour, comparaître comme partie à une instance engagée en vertu de l'article 14.

Voici une liste des demandes déposées devant les tribunaux en vertu de la LPRPDE du 1^{er} janvier 2001 jusqu'au 31 décembre 2002 :

Mathew Englander c. Telus Communications Inc.
N° de dossier de la Cour fédérale du Canada : T-1717-01

Il s'agit de la première demande qui a été déposée à la Cour fédérale aux termes de la LPRPDE. M. Englander soutient que Telus utilise et communique les noms, adresses et numéros de téléphone de ses clients figurant dans les pages blanches de son annuaire et ailleurs, à l'insu de ses clients et sans avoir obtenu leur consentement. En outre, Telus impose de manière inappropriée des frais aux clients qui demandent la « non-publication » de leur numéro de téléphone. M. Englander soutient que ces mesures prises par Telus sont contrairement aux paragraphes 5(1) et (3) de la LPRPDE, ainsi qu'à plusieurs clauses de l'annexe 1 de la Loi.

État de la situation

Cette demande a fait l'objet d'un non-lieu le 2 juin 2003.

EXAMENS ET PRATIQUES EN MATIÈRE DE VIE PRIVÉE

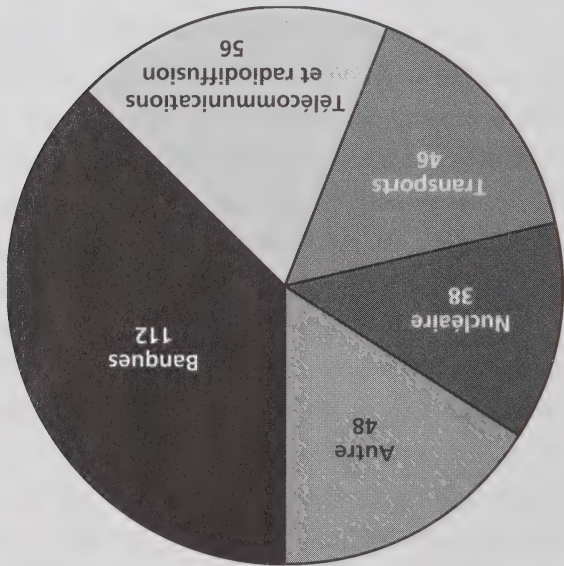
La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) autorise le commissaire à vérifier la conformité des organisations du secteur privé avec la Loi s'il a des motifs raisonnables de croire qu'elles contreviennent à la Loi ou qu'elles ne respectent pas une des recommandations énoncées dans l'annexe 1 (les dix principes). La Direction des examens et des pratiques en matière de vie privée du Commissariat effectuera des examens et des vérifications de conformité, aux termes de l'article 18 de la LPRPDE, en tenant compte des objectifs et des critères de vérification standard reconnus. Au cours de la période couverte par le présent rapport, un certain nombre de questions ont été portées à l'attention de l'ancien commissaire, qui ont été résolues avec succès sans qu'on n'ait eu besoin d'effectuer une vérification. Par exemple, le personnel du Commissariat a rencontré et conseillé des représentants d'une association d'entreprises sur la viabilité du consentement direct et le contenu proposé d'un tel formulaire de consentement. Nous avons offert des conseils à une entreprise en ce qui concerne l'utilisation du NAS comme identificateur et l'utilisation du consentement négatif. De plus, nous avons procédé à un examen et une analyse d'ensemble de la politique sur la protection des renseignements personnels d'une société.

Hormis ces questions, l'ancien commissaire n'a été au courant d'aucun autre problème qui aurait pu lui donner des motifs suffisants pour entreprendre une vérification en vertu de la loi.

Néanmoins, la Direction des examens et des pratiques en matière de vie privée a pris part à des consultations avec les organisations du secteur privé qui sont assujetties à la LPRPDE et leur a offert des conseils. Elle a également apporté son aide aux organisations qui ne sont pas régies par la Loi mais qui se préparent pour le 1^{er} janvier 2004, lorsque la Loi commencera à s'appliquer à elles.

L'ancien commissaire était convaincu que la banque avait réagi de manière rapide et appropriée face à cette situation délicate.

Nombre de plaintes selon le secteur
1^{er} janvier 2002 au 31 décembre 2002



Demandes de renseignements en vertu de la LPRPDE
1^{er} janvier 2002 au 31 décembre 2002 : 8 381

Nous essayerons de fournir une répartition de ces demandes de renseignements par thème dans les prochains rapports annuels

nom des clients ni d'autres renseignements pouvant les identifier. L'entreprise a signé un contrat de non-divuligation avec le cabinet, qui exigeait que le cabinet détruise tous les renseignements qu'il recueillait une fois que les résultats du sondage auront été compilés.

L'ancien commissaire était heureux d'apprendre qu'il a été déterminé que la compagnie de téléphone se conformait à une exigence du CRTC voulant que celle-ci mesure régulièrement la qualité du service relativement à l'exactitude des services de l'assistance-annuaire.

Trouvaille près d'une benne à ordures

Une banque a alerté le Commissariat que des documents confidentiels sur des clients avaient été retrouvés dans une benne à ordures située près de la succursale qui avait fermé quelque temps auparavant. L'édifice avait été loué à un nouveau locataire et était en rénovation. Apparemment, les personnes qui effectuaient les réparations avaient trouvé les documents au cours des travaux, puis les avaient jetés. Après avoir eu vent de l'incident, les médias ont récupéré certains documents de la benne à ordures.

La banque a réagi rapidement aussitôt qu'elle a pris conscience de la situation, en récupérant tous les documents qui se trouvaient dans la benne et ceux que les journalistes avaient entre les mains ; puis elle s'est assurée qu'il ne restait aucun autre document de la banque dans l'édifice. La banque a également informé tous les clients touchés, en personne ou par écrit, de l'incident et des mesures qu'elle avait prises pour récupérer les documents. De plus, la banque s'est excusée auprès de chaque client et leur a assuré que tous leurs renseignements avaient été récupérés.

Il a été déterminé que la succursale en question avait été fusionnée avec une autre succursale et qu'une entreprise privée sous contrat avec la banque avait été mandatée pour trier et traiter tous les dossiers. La banque a établi des procédures destinées à cet effet, mais l'entreprise privée ne les avait pas suivies correctement, ce qui a eu pour effet le fait que certains documents n'étaient pas bien classés et qu'ils avaient été jetés de façon inappropriée. La banque a par la suite clarifié les procédures avec l'entreprise privée.

- Si les renseignements doivent être communiqués à des tierces parties, les parties doivent être identifiées par nom ou par catégorie.

- L'organisation doit stipuler ses fins en se conformant entièrement aux principes 4.2, 4.2.3, 4.3.1 et 4.3.2 et aux attentes raisonnables de la personne jugées pertinentes en vertu du principe 4.3.5. Plus particulièrement, les fins déterminées doivent être directement portées à l'attention de la personne, oralement ou par écrit, au moment de la collecte de renseignements personnels (par exemple, lors du processus d'abonnement, de demande ou d'inscription) ; en termes clairs, précis et sans équivoque ; dans un format facile à lire (lorsqu'il s'agit d'un texte) ; et d'une façon permettant à la personne de comprendre de quelle manière exactement les renseignements personnels seront utilisés ou communiqués.

- L'organisation doit offrir une formule d'option de refus appropriée, c'est-à-dire une possibilité et une procédure convenables pour retirer un consentement. La formule doit être expliquée à la personne au moment de la collecte de renseignements personnels à son sujet et devrait être peu coûteuse, facile à exécuter et avec effet immédiat quant au retrait du consentement. Si possible, elle devrait comprendre un numéro de téléphone sans frais.

INCIDENTS VISÉS PAR LA LPRPDE

Vérification des appels téléphoniques

Un journaliste a communiqué avec le Commissariat au sujet d'un sondage qu'effectuait un cabinet de recherche pour le compte d'une compagnie de téléphone. Il a semblé que l'entreprise recueillait auprès des clients des renseignements à propos de leurs appels téléphoniques.

Le cabinet de recherche avait signé un contrat avec la compagnie de téléphone afin d'effectuer des vérifications au hasard à des fins d'assurance de la qualité. La compagnie de téléphone a fourni au cabinet une liste des numéros de téléphone de clients qui avaient téléphoné pour obtenir de l'assistance en composant le « 0 » ou le « 411 ». Le cabinet n'a pas reçu le

meilleure pour rester fidèle à l'esprit de la Loi. On encourage fortement les organisations à adopter exclusivement cette forme de consentement.

- Le consentement positif ou actif à des fins secondaires est nécessaire dans des situations où les renseignements personnels sont de nature sensible ou dans des situations où il existe une grande probabilité pour que les renseignements deviennent de nature sensible dans le contexte des activités de gestion des renseignements.

- Puisque la Loi indique que les renseignements personnels de nature financière ou médicale doivent presque toujours être considérés comme étant de nature sensible, on présume que ces types de renseignements devront presque toujours exiger un consentement positif. Cependant, puisque la Loi stipule également que tout renseignement personnel peut être de nature sensible dans un contexte donné, aucune autre tentative ne devrait être faite pour définir précisément la notion de sensibilité. Le contexte devrait plutôt être considéré dans chaque cas dans le but de déterminer le potentiel de sensibilité.

- Les deux principales considérations permettant de déterminer le potentiel de sensibilité des renseignements personnels sont l'intention de communiquer les renseignements à des tierces parties et l'intention de classer ou autrement dit de traiter les renseignements selon des critères personnels.

- Le consentement négatif ou passif, également connu sous le nom de consentement présumé, même si celui-ci représente la forme la plus faible et la moins préférable, est reconnu en vertu de la Loi comme étant acceptable dans certaines circonstances. La portée des circonstances dans laquelle cette forme de consentement est permise demeure limitée.

- L'utilisation par une organisation de la forme négative ou passive de consentement à des fins secondaires sera justifiée seulement sous les conditions suivantes :

- Les renseignements personnels doivent s'avérer, démonstration faite, de nature et d'un contexte non sensible et doivent être déterminés par élément ou par catégorie.

efforts entrepris par la banque pour obtenir un consentement éclairé auprès des personnes désirant ouvrir un compte ne satisfaisaient aucunement aux exigences de la Loi ni les attentes raisonnables de la personne. Dans la lettre de conclusions, l'ancien commissaire a émis des commentaires sur divers documents utilisés par la banque afin de communiquer ses fins, ainsi que sur la nature et la portée du non respect de la Loi dans ce cas :

« Les termes ... sont tellement vagues qu'ils sont presque incompréhensibles, à moins qu'on les interprète comme voulant dire que la banque a l'intention d'utiliser les renseignements personnels comme bon lui semble et de les communiquer à qui elle veut. Ce qui constituerait à peine une fin à laquelle aucune personne raisonnable ne s'attendrait et qu'aucune personne raisonnable ne jugerait appropriée en aucun cas. » [traduction]

En revanche, sur une note positive, on devrait noter que, dans le cas de la première banque, l'ancien commissaire a complimenter la banque sur son approche concernant l'obtention du consentement éclairé de la part des personnes désirant ouvrir un compte. Dans le cas des personnes faisant une demande directement dans une succursale, la procédure de demande de cette banque exige que l'on s'assure avec la personne, qu'on lui donne immédiatement les renseignements appropriés sur la protection des renseignements personnels, que l'on attire son attention particulièrement sur les déclarations concernant les fins secondaires de marketing, qu'on lui demande si elle consent ou non à des pratiques de marketing particulières, que l'on prenne note de ses réponses et qu'on les respecte. Nous considérons de telles procédures comme exemplaires, presque autant que la forme positive de consentement que nous préférons.

Consentement à des fins secondaires

Ce qui suit constitue un sommaire des délibérations menées jusqu'à ce jour dans des cas relatifs au consentement à des fins secondaires :

- Le consentement positif ou actif doit toujours être préféré comme la forme de consentement la plus forte, la plus respectueuse des personnes et la

Compte tenu de ces éléments et après enquête sur les politiques et les pratiques réelles des organisations, l'ancien commissaire a conclu que deux des plaintes étaient fondées et que deux ne l'étaient pas. Il a conclu que la compagnie de télécommunications ne communiquait aucun renseignement tel qu'allégué, puisque le CRTC l'interdit. L'une des banques communiquait effectivement des renseignements à des fins secondaires de marketing tel qu'allégué, mais l'ancien commissaire a conclu que la banque faisait dans l'ensemble des efforts raisonnables pour informer les personnes désirant ouvrir un compte de la pratique, pour obtenir leur consentement et pour leur offrir une possibilité d'exercer l'option de refus.

Dans le cas des plaintes fondées, la non conformité avec la *Loi* du programme pour clients réguliers était largement due à une incohérence des procédures d'inscription. Cependant, le cas de la seconde banque était plus sérieux. Les

- Si les fins sont déterminées par écrit, la personne ne devrait pas être obligée de les lire en caractères minuscules dans des passages denses.
- Les fins devraient être stipulées dans un langage clair, simple et compréhensible pour le consommateur ordinaire et de façon bien détaillée afin que celui-ci puisse apprécier la nature et l'étendue de la collecte, de l'utilisation et de la communication envisagées. (Ces attentes sont soutenues par le principe 4.3.2, qui stipule que les fins doivent être énoncées de telle façon que la personne puisse de manière raisonnable comprendre de quelle manière les renseignements seront utilisés ou communiqués).
- Si les fins sont déterminées par écrit, la personne ne devrait pas être obligée de les lire en caractères minuscules dans des passages denses.

Les principes 4.2.3 et 4.3.1 de la *Loi*, qui stipulent que la détermination des fins et l'obtention du consentement soient directes et coïncident avec la collecte des renseignements personnels).

informées des fins secondaires, les organisations n'avaient aucune base valide de présumer le consentement des personnes à de telles fins. Selon la seconde allégation, en dépit du fait qu'elles se fiaient à la formule de consentement de l'option de refus, les organisations n'offraient pas aux personnes des possibilités raisonnables d'exercer l'option de refus dans le cadre du marketing mené par les tierces parties.

*Pour nous, ces
suppositions
traduisaient clairement
des « attentes » de la
part du plaignant.*

Aussi intéressantes que les allégations elles-mêmes furent les suppositions sous-jacentes que le groupe d'intérêt avait présentées dans une déclaration de principe soutenant les plaintes. Pour nous, ces suppositions traduisaient clairement des « attentes » de la part du plaignant. Avant de déterminer si les organisations en question s'étaient conformées ou non aux dispositions pertinentes de la Loi sur le consentement, nous avons jugé qu'il est prudent d'examiner la question de savoir si les attentes du groupe au sujet du consentement étaient elles-mêmes raisonnables au regard de la Loi.

Après les avoir analysées, l'ancien commissaire a conclu que les attentes du groupe étaient entièrement raisonnables. Plus particulièrement, il a jugé qu'il est raisonnable d'attendre des organisations qui utilisent ou qui communiquent des renseignements personnels à des fins secondaires ce qui suit :

- Ce n'est pas assez de déterminer des objectifs dans des documents portant sur la politique en matière de protection des renseignements personnels et de les rendre largement disponibles. Une organisation devrait porter ses fins secondaires directement à l'attention de la personne au moment de recueillir les renseignements personnels. À l'occasion d'une demande ou d'un abonnement, par exemple, la personne devrait recevoir les renseignements nécessaires et on ne devrait pas lui référer des sources qui ne sont pas immédiatement disponibles. (Ces attentes sont soutenues par

Les plaintes consistaient en deux allégations principales. Selon la première, les organisations ne faisaient pas d'efforts raisonnables pour informer leurs clients que leurs renseignements pourraient être communiqués à des tiers parties à des fins secondaires de marketing, c'est-à-dire à des fins en sus de celles pour lesquelles il a été nécessaire de recueillir les renseignements au départ. Le plaignant a allégué que si les personnes n'étaient pas dûment

concernant. pour communiquer à des fins de marketing des renseignements personnels les n'avaient pas obtenu de consentement valide et informé auprès des personnes relativement semblables et alléguait que les organisations en question offrent un programme pour les clients réguliers. Toutes les plaintes étaient deux banques, une compagnie de télécommunications et une entreprise qui Une personne a déposé une plainte au nom d'un groupe d'intérêt à l'encontre

matière de consentement. formuler une position générale sur ce qu'une personne devait s'attendre en une série de plaintes ont été portées de sorte que nous avons jugé utile de ainsi que leur portée réelle. Heureusement, dès l'entrée en vigueur de la Loi, commissaire de déterminer le caractère raisonnable des attentes du plaignant, contexte de toute plainte liée au consentement, il revient souvent au Elle nous laisse plutôt la tâche ardue d'interpréter cette disposition. Dans le

Mais elle n'approuvait pas le sujet. L'raisonnables de la personne sont pertinentes en matière de consentement.

Un groupe d'intérêt propose des « attentes » en matière de consentement

insuffisantes, vagues et trompeuses qui lui sont fournies. Au lieu de cela, de mon point de vue, loin d'offrir une compréhension raisonnable de la manière dont les renseignements personnels seront utilisés ou communiqués, les documents du sondage ont uniquement servi à tromper les personnes sur les véritables objectifs des sondages et à nuire à l'équité de la collecte des renseignements personnels par l'entreprise. » [traduction]

En réalité, l'entreprise a une politique officielle écrite, affichée sur son site Web, sur la protection des renseignements personnels concernant ses sondages effectués auprès des ménages. Cette politique détermine relativement bien les fins réelles de la collecte des renseignements de sondage. Cependant, cette politique n'est non seulement pas intégrée à la documentation du sondage envoyée par la poste aux ménages, mais elle n'est pas non plus accessible de façon raisonnable aux ménages. La documentation du sondage ne mentionne même pas l'existence du site Web, encore moins l'existence de cette politique.

Ce qui nous a troublés particulièrement était le grand écart concernant la conformité avec la Loi, entre le site Web et la documentation du sondage, ainsi que les conséquences de cet écart. Dans la lettre de conclusions, l'ancien commissaire a soulevé les préoccupations suivantes :

« Pourquoi [l'entreprise] indiquerait-elle de manière raisonnablement claire dans une politique sur la protection des renseignements personnels, tenue à l'écart et non annoncée, mais de façon nébuleuse dans la documentation sur le sondage remise aux personnes, que les renseignements personnels des répondants seraient communiqués à des tierces parties à des fins de marketing? Pourquoi dans les documents de sondage, [l'entreprise] explique-t-elle les fins en des termes aussi restreints que la recherche de faits, la collecte d'opinions et l'amélioration de la qualité des produits et relogue dans un document, dont personne ne pourrait normalement prendre connaissance, les autres fins de marketing direct par des tierces parties? En réalité, pourquoi [l'entreprise] ferait l'effort de formuler une politique en matière de protection de renseignements personnels plus ou moins conforme à la Loi pour ne pas attirer ensuite l'attention de chaque répondant à cet égard au moment où cela importe réellement, en cachant, de fait, la politique aux consommateurs? » [traduction]

« En résumé, j'ai de la difficulté à comprendre cet écart, excepté en termes de supercherie. [L'entreprise] a suggéré que ses documents de sondage servaient à susciter une attente raisonnable de communication aux tierces parties et de marketing direct de leur part. Cependant, je ne comprends pas comment une personne peu méfiant pourrait supposer une telle fin à partir des indications

sensible (en l'occurrence, plusieurs questions concernent la santé et les finances personnelles), la formule de consentement de l'« option d'acceptation » devrait être utilisée dans de telles circonstances. Mais la formule de consentement consiste à cocher une des deux cases, « Oui » et « Non », ce qui rend plutôt ambiguë la formule de consentement recherchée. Cependant, ce qui se passe en réalité, dans les cas assez fréquents où le répondant ne coche aucune des cases, c'est qu'on présume que la personne consent à recevoir d'autres envois. Ainsi, l'entreprise utilise la formule de consentement de l'« option de refus » dans une situation qui fait clairement appel à une « option d'acceptation ».

La documentation du sondage mentionne également que des entreprises ont commandé ce sondage. Cependant, elle ne nomme pas ces entreprises, ni ne suggère de façon perceptible que ces entreprises anonymes sont des agences de vente directe ou qu'ils ont en effet commandé à l'entreprise d'études de marché ce sondage dans le but de recueillir des renseignements personnels sur d'éventuels consommateurs. En réalité, il n'existe rien dans la documentation qui pourrait donner aux ménages des raisons de croire que le sondage n'est rien d'autre de ce qu'il prétend être à première vue, c'est-à-dire une étude de marché axée sur la recherche de faits et d'opinions, qui vise à améliorer les produits.

En fonction d'une telle description, les répondants pourraient s'attendre à ce que les entreprises qui ont commandé le sondage en reçoivent les résultats sous forme de données analytiques cumulatives et anonymes. Mais les répondants n'ont aucune raison légitime de s'attendre, et ils ont toutes les raisons d'en être insultés, à ce que leur participation au sondage ait pour effet de les rendre sujets à des efforts de marketing direct non désirés qui portent atteinte à la protection de leur vie privée par des tierces parties qui ont eu connaissance de renseignements personnels de nature sensible les concernant.

Cela peut sembler paradoxale pour certains que, malgré le cas accablant contre l'entreprise d'études de marché en raison de ces allégations et de bien d'autres, nous étions principalement préoccupés par les signes évidents de la *conformité* de l'entreprise avec la Loi.

Si une organisation

a l'intention de

transmettre les

renseignements qu'elle

recueille directement à

des commerçants, elle

doit le mentionner...

parties qui avaient commandé le sondage en question. Celles-ci essayeront par la suite de vendre leurs produits aux répondants du sondage en leur envoyant directement de la publicité en fonction des renseignements qu'ils ont fournis dans les réponses aux questionnaires.

La LPRPD stipule qu'une organisation doit énoncer les vrais motifs pour lesquels elle recueille des

renseignements personnels. Elle stipule également que le consentement à la collecte de renseignements personnels ne doit pas être obtenu par une supercherie. Si une organisation a l'intention de transmettre les renseignements qu'elle recueille directement à des commerçants, elle doit le mentionner, en termes clairs et énoncés de façon à être raisonnablement compris par les personnes. Dans la documentation du sondage en question, il n'existe aucune déclaration explicite ni une aucune insinuation compréhensible et raisonnable informant les répondants que leurs renseignements personnels seraient communiqués à des tierces parties.

Le questionnaire sollicite le consentement des répondants en vue d'autres envois et offres postaux, mais ne mentionne pas de quelles sources proviendront ces envois. En l'absence de telle indication mentionnant que l'entreprise de sondages a l'intention de partager l'adresse postale du répondant avec d'autres expéditeurs éventuels, l'inférence la plus raisonnable serait que tous les envois et les offres proviendront de la même source que celle qui était à l'origine de la collecte, c'est-à-dire de l'entreprise de sondages elle-même.

De plus, la formule de consentement pose en elle-même un problème. Compte tenu du fait que les questions du sondage sont de nature hautement

Cependant, les sondages avaient réellement pour objectif de vendre des produits aux répondants du sondage. Ce que l'entreprise avait principalement l'intention de faire avec les renseignements qu'elle recueillait était de compiler les listes d'envoi personnalisées qui, par la suite, seraient données aux tierces

tout dans le but d'améliorer la qualité, la durée et la valeur des produits. compréhension des « préférences et des attitudes des consommateurs », le en terme de recherche des « faits », de collecte « d'opinions » et de accompagner les questionnaires explique les objectifs du sondage strictement ménages parmi diverses catégories de produits. La documentation qui Canada. Les questionnaires comportent des questions sur les présences des des « sondages sur des produits grand public » aux ménages à travers le Cette entreprise envoie par la poste des questionnaires pour ce qu'elle appelle plainte à l'encontre d'une entreprise d'études de marché.

C'est une chose de peu informer les personnes des fins pour lesquelles leurs renseignements personnels pourraient être utilisés, tel que l'ont fait trois des organisations mentionnées plus haut. C'est une autre chose de mal les informer de façon délibérée, tel que nous l'avons conclu dans le cas d'une

Un cas de supercherie

dont l'entreprise a fait preuve. Nous étions convaincus qu'Air Canada avait répondu de façon appropriée à nos recommandations et nous sommes heureux de l'esprit de coopération site Web d'Aéropian.

leur prochain état de compte. De plus, la politique allait être affichée sur le membres actifs du programme recevraient copie de la politique révisée avec Aéropian, Air Canada a aussi dressé un plan très précis selon lequel tous les En ce qui concerne la question relative à la consultation de tous les membres méthode facile pour exercer cette option.

de leurs points Aéropian peuvent le stipuler et il fournit aux membres une que leurs renseignements personnels ne soient utilisés que pour le rachat • elle énonce explicitement et clairement que les membres qui souhaitent

personnalisés suivant des critères de nature potentiellement sensible. L'ancien commissaire a ainsi déclaré dans ses lettres :

« Bien que je considère que la pratique qui consiste à partager les renseignements des membres du programme à des fins de publicité de produits, de services et de promotions spéciales soit en elle-même acceptable, je suis persuadé qu'une personne raisonnable ne s'attendrait pas à ce qu'une telle pratique s'étende à la « fabrication sur mesure » de l'information suivant les intérêts, les usages et les préférences de nature potentiellement sensible de la personne sans son consentement explicite. » [traduction]

L'ancien commissaire a conclu qu'il avait été inapproprié pour Air Canada de recourir au consentement négatif ou à l'option de refus dans le cadre des politiques et des pratiques de partage d'information d'Aéropian, telles que décrites dans la brochure.

À son honneur, Air Canada a pris très au sérieux les conclusions et les recommandations de l'ancien commissaire. Grâce à quelques conseils apportés par le Commissariat dans un processus qui nous a semblé à la fois positif et fructueux, la compagnie a entrepris de repenser et de ré-écrire sa politique de partage d'information dans le cadre d'Aéropian. Nous avons examiné le produit fini et vérifié que la politique traite à présent de nos préoccupations des façons suivantes :

- elle explique aux membres Aéropian, en termes clairs et compréhensibles, les buts de la collecte, de l'utilisation et de la communication des renseignements personnels dans le cadre du programme ;
- elle explique clairement qu'Aéropian ne recueille aucun renseignement sur les opérations en fonction desquelles les membres accumulent des points dans le cadre du programme ;

- elle précise qu'Aéropian ne fournit pas de profil personnalisé des membres aux entreprises partenaires ou à d'autres tierces parties, et précise également que tout renseignement fourni aux partenaires ne peut être utilisé qu'à des fins liées au programme Aéropian ;

consentement, qui rejette injustement la responsabilité sur le mauvais parti et reflète au mieux un respect de pure forme de ce qui est sans doute le principe le plus fondamental de la *Loi*. Nous préférons que les organisations adoptent une approche exclusivement positive ou fondée sur l'« option d'acceptation » – une approche beaucoup plus respectueuse selon laquelle on estimerait qu'une personne a consenti seulement si elle a catégoriquement dit « oui » à une proposition.

Par ailleurs, le Commissariat est aussi conscient que l'option de refus est une forme de consentement expressément permise par la *Loi* dans certaines circonstances – notamment, lorsque les renseignements personnels sont manifestement de nature non sensible. Le problème dans ce cas est que la *Loi* ne définit pas précisément la notion de sensibilité. Bien qu'elle énonce que les renseignements financiers et médicaux d'une personne doivent presque toujours être considérés comme étant sensibles, elle suggère que n'importe quel renseignement peut être sensible selon le contexte. Par conséquent, en ce qui concerne les plaintes relatives à Aéroplan, la tâche du Commissariat consistait essentiellement à évaluer le contexte. Autrement dit, l'ancien commissaire devait déterminer si les circonstances justifiaient le recours par Air Canada à l'option de refus.

Dans ses lettres de conclusions, l'ancien commissaire a expressément fait état de son intention de toujours établir de limites strictes en ce qui concerne les circonstances dans lesquelles l'option de refus pourrait être jugée appropriée. Il a aussi clairement exprimé son intention de se laisser guider dans de telles délibérations par la prise en compte en bonne et due forme de la sensibilité des renseignements et des attentes raisonnables de la personne. C'est sur la base de ces considérations que la brochure d'Aéroplan sur la protection des renseignements personnels s'est avérée non conforme à la *Loi*.

Le libellé de la brochure ne montre pas que les situations de partage de l'information décrites étaient strictement de nature non sensible ou d'un contexte non sensible. Deux des situations étaient particulièrement sensibles. Les trois autres semblaient par leur description permettre un marketing de grande envergure à l'endroit des membres en fonction de renseignements

À l'instar de la plupart des autres personnes impliquées dans la protection de la vie privée et, en fait, comme la plupart des consommateurs avertis, nous avons une très mauvaise opinion de l'abonnement par défaut qu'utilisent les organisations pour le traitement des renseignements personnels. Le Commissariat considère que l'option de refus est une forme médiocre de consentement à moins qu'elle n'entrepreneue des démarches pour le refuser.

« consentement négatif » ou « option de refus ». Elle correspond aux pratiques de marketing de l'« abonnement par défaut » que les consommateurs ont vite fait de condamner dans le passé. En effet, une telle pratique est fondée sur la présomption – la personne est présumée donner son

présent connue sous le nom de Cette forme de consentement est à l'information. façons dont Air Canada comptait partager les renseignements personnels des membres Aéroplan dans le cadre du programme. Chaque description était accompagnée d'une case à cocher et le membre du programme devait cocher la case seulement s'il ne consentait pas à ce que ses renseignements personnels soient partagés de la manière décrite. Tout membre du programme qui cochant une ou plusieurs des cinq cases devait ensuite retourner la brochure par la poste à l'entreprise afin de signifier le refus de consentement. Inversement, tout membre du programme qui ne retournerait pas la brochure était considéré comme un membre ayant consenti aux cinq

À l'instar de la plupart des autres personnes impliquées dans la protection de la vie privée et, en fait, comme la plupart des consommateurs avertis, nous avons une très mauvaise opinion de l'abonnement par défaut qu'utilisent les organisations pour le traitement des renseignements personnels.

combustibles nucléaires et n'aurait plus été en mesure de poursuivre ses activités liées aux produits nucléaires, ce qui aurait entraîné des pertes financières considérables et des mises à pied. Dans ces circonstances, nous avons déterminé qu'il était entièrement raisonnable de la part de l'entreprise de se conformer à la directive et, ce faisant, de recueillir des renseignements personnels auprès des employés afin d'effectuer des vérifications de sécurité.

Aéropian : l'option de refus n'est pas suffisante

Lorsque Air Canada a envoyé par la poste des brochures sur la protection des renseignements personnels à 60 000 membres Aéropian, plusieurs ont déposé une plainte au Commissariat.

Les personnes qui se sont plaintes au Commissariat n'étaient pas du tout contrariées par l'effort entrepris par la compagnie dans le but d'obtenir leur consentement à propos des pratiques de partage d'information en vertu du programme Aéropian. Elles s'opposaient toutefois à ce qu'on rejette sur *elles* la responsabilité d'informer Air Canada si elles *ne* consentaient pas aux pratiques énoncées dans la brochure. Elles n'appréciaient pas non plus que l'entreprise présume, dans l'intervalle, qu'elles y consentaient.

L'ancien commissaire a conclu qu'Air Canada ne s'est pas conformé pas à la *LPRPD* et que les plaintes étaient fondées.

Les 60 000 brochures ne représentaient qu'environ un pour cent du nombre total de membres Aéropian à ce moment. Dans ses lettres de conclusions, l'ancien commissaire a fait remarquer que la *Loi* exige que les organisations respectent les droits à la vie privée de chaque personne et ne permet pas une conformité de pure forme. Étant donné qu'Air Canada avait en fait laissé 99 p. 100 des membres Aéropian dans l'ignorance au sujet de sa politique et de ses pratiques de partage d'information, l'ancien commissaire a jugé que la démarche que la compagnie a entreprise dans le but d'obtenir ce consentement avait été entièrement inadéquate.

Même si tous les membres du programme avaient été consultés, la brochure même n'utilisait pas une formule de consentement appropriée. Elle décrivait cinq

Certains employés étaient mécontents et se sont plaints au Commissariat. Ils avaient l'impression de n'avoir aucun autre choix – s'ils refusaient, ils perdaient leur emploi. S'ils y consentaient mais qu'ils ne satisfaisaient pas à la vérification de sécurité, ils perdaient leur poste actuel et seraient réaffectés éventuellement à des postes moins bien payés. Ils avaient le sentiment, dans ces circonstances, que leur consentement était forcé.

L'ancien commissaire devait déterminer si l'entreprise avait recueilli les renseignements personnels de ses employés après les en avoir informés et obtenu leur consentement en vertu du principe 4.3 de la *LPRPDE*. Il était clair que les employés étaient au courant de cette collecte. Mais leur consentement était-il volontaire? Dans ses lettres de conclusions, l'ancien commissaire a jugé la question de la façon suivante :

« [l'entreprise] vous a expressément demandé de donner votre consentement et il n'appartenait qu'à vous de le faire ou non. Le fait qu'il peut en découler des conséquences négatives dans l'un ou l'autre cas ne change rien au fait qu'on vous avait offert un choix en l'espèce. Le fait de refuser de consentir à la collecte de renseignements personnels peut très souvent entraîner des conséquences négatives pour la personne. Mais dans ce cas, comme dans la plupart des décisions prises dans la vie qui risquent d'avoir des conséquences négatives, la pression que vous pouvez ressentir au sujet du consentement à donner dans le cadre de la collecte ne constitue pas une contrainte. En vertu de la Loi, la principale considération n'est pas de savoir si des conséquences négatives peuvent découler ou non du refus d'une personne de donner son consentement, mais plutôt de savoir si la collecte est elle-même raisonnable ou non. » [traduction]

Était-il raisonnable de recueillir des renseignements personnels à des fins d'autorisation de sécurité, comme stipulé au paragraphe 5(3) de la *Loi*? L'ancien commissaire a conclu qu'il était entièrement raisonnable de la part de l'organisme fédéral d'imposer à ses titulaires de permis des exigences accrues en matière de sécurité, compte tenu des préoccupations considérablement aiguës au sujet d'éventuels actes de terrorisme dans les installations nucléaires. Si l'entreprise ne s'était pas conformée à la directive de l'organisme fédéral, elle aurait perdu sa licence de production de

renseignements personnels ni qu'elle ait une discussion avec l'organisation concernant ses raisons. En d'autres termes, les renseignements personnels ne peuvent être mis à rancun.

Compte tenu de ces conclusions, la consigne essentielle pour les organisations en ce qui concerne les droits est celle-ci : le recouvrement des coûts ne s'applique pas aux demandes d'accès à l'information.

Une autorisation de sécurité devient une condition d'emploi

L'a protection des sites nucléaires contre les attaques terroristes est l'objet d'une sérieuse préoccupation surtout depuis le 11 septembre 2001. L'organisme fédéral qui supervise les opérations de toutes les installations nucléaires au Canada a répondu à la menace terroriste en ordonnant à ces titulaires de permis de mettre en œuvre des mesures de sécurité améliorées. L'une des nouvelles mesures en place consiste à limiter l'entrée aux installations nucléaires aux personnes ayant l'autorisation de sécurité appropriée. Si un titulaire de permis refuse de se conformer à cette nouvelle mesure, l'organisme fédéral révoquera sa licence de production.

Une division des produits nucléaires de l'entreprise a informé ses employés de la nouvelle exigence en matière de sécurité et leur a également demandé de consentir à une vérification de sécurité. Chaque employé de la division a reçu une trousse d'information accompagnée de formulaires de consentement qui précisaient le type de renseignements qui seraient recueillis, le but de la collecte et le nom de l'agence responsable de la collecte. Les employés ont aussi été informés que l'agence chargée de la collecte des renseignements personnels était liée par une entente concernant la confidentialité.

Afin d'obtenir une autorisation de sécurité, les employés comptant plus de dix ans de service devaient satisfaire à une vérification du casier judiciaire. Les employés comptant moins de dix ans de service devaient satisfaire à une vérification complète de leurs antécédents, notamment les antécédents en matière d'emploi, les compétences professionnelles et les références personnelles, ainsi qu'à la vérification de leur casier judiciaire.

Ces deux cas représentent un bon exemple de la manière dont le secteur privé s'adapte aux attentes des plaignants étaient impliqués dans des disputes avec leur banque respective concernant un prêt lorsqu'elles répondent aux demandes. Mais quels montants sont considérés comme étant raisonnables? Cette question a été traitée dans deux cas où les plaignants accusaient les organisations d'imposer des droits excessifs.

Les plaignants étaient impliqués dans des disputes avec leur banque respective concernant un prêt lorsqu'elles avaient contracté. Les deux personnes ont demandé à avoir accès à leurs renseignements personnels. Les banques ont répondu en leur exigeant des droits de 150 \$ et de 200 \$ respectivement, afin de couvrir les coûts de traitement des documents en question. La première personne voulait savoir ce qu'elle allait obtenir pour son argent et lorsqu'elle en a été informée, elle a décidé de porter plainte. La deuxième personne perçoit un revenu fixe et ne pouvait se permettre de payer un tel montant pour obtenir ses renseignements personnels.

Ces deux cas représentent un bon exemple de la manière dont le secteur privé s'adapte aux attentes de la Loi. On a rappelé aux banques que le principe 4.9.4 de la LPRPD stipule qu'une organisation qui reçoit une demande de communication de renseignements personnels doit y répondre et ne peut exiger, pour ce faire, que des droits minimes. Cela a eu pour effet qu'une des banques a accepté de communiquer les renseignements à aucun frais, tandis que l'autre a imposé des frais nominaux de 10 \$.

De plus, la position de la banque dans le cas du premier plaignant semblait être basée non seulement sur une question de recouvrement des coûts, mais également sur son désir de rencontrer le client afin de discuter de la dispute qui avait donné lieu au départ à la demande d'accès aux renseignements. Cependant, nous avons signifié à la banque que la Loi n'exige pas qu'une personne explique les raisons pour lesquelles elle souhaite avoir accès à ses

aérien de lui communiquer l'itinéraire du plaignant. Convaincu que la demande du ministre était conforme à l'article 7(3)(c.1)(iii) de la Loi, le transporteur aérien a dûment communiqué les renseignements. Cet alinéa permet à une organisation de communiquer des renseignements au sujet d'une personne à une institution gouvernementale à des fins d'administration de la loi.

Il y avait cependant un seul problème. Le ministre n'a pas invoqué la bonne directive comme autorité légitime. Même si par la suite le ministre a reconnu son erreur, il a maintenu qu'il avait tout de même l'autorité légitime de recueillir ces renseignements en vertu d'une autre loi.

Nous avons convenu que le ministre avait l'autorité légitime. Toutefois, nous étions préoccupés par le fait que le ministre avait commis une erreur au départ et que le transporteur aérien avait omis de vérifier l'exactitude de l'autorité invoquée par le ministre. Même si le transporteur aérien a communiqué les renseignements de bonne foi, une organisation a l'obligation d'être vigilante en ce qui a trait à la vérification des pouvoirs invoqués par les organisations gouvernementales avant de communiquer des renseignements personnels. Dans sa lettre de conclusions, l'ancien commissaire a déclaré à ce propos :

« ...dans les cas de demandes de communication de renseignements personnels, je considère qu'il revient à toute organisation du secteur privé de ne pas accorder foi de prime abord aux demandes d'une organisation gouvernementale, mais plutôt d'être vigilante en ce qui a trait à la vérification des pouvoirs invoqués. » [traduction]

Frais d'accès : devriez-vous payer pour avoir accès à vos propres renseignements?

Le fait de répondre à des demandes d'accès aux renseignements personnels peut occasionner des coûts pour une organisation. Cela devrait-il occasionner également des coûts pour les personnes? En réalité, il existe une disposition dans la Loi qui permet aux organisations d'imposer des droits

Afin donc de répondre à la question soulevée ci-dessus, un FAL devrait suivre, dans les cas d'une suspension de compte, ce nous avons recommandé comme pratiques exemplaires dans le cas en question :

- Cesser la collecte, le stockage et le refus d'accès aux messages électroniques destinés aux détenteurs des comptes suspendus.
- Adopter plutôt une pratique qui consiste à détourner les messages électroniques et à les retourner aux expéditeurs accompagnés d'un avis les informant que le message n'a pu être délivré.

- Prendre des dispositions pour donner accès au détenteur d'un compte suspendu à tous les messages électroniques reçus par l'entreprise, mais qui n'avaient pas été récupérés par le client au moment de la suspension.

Assurez-vous de vérifier ces pouvoirs qu'invoque le gouvernement

Les souvenirs de vacances d'une personne ont été gâchés lorsqu'elle a découvert que le transporteur aérien avec lequel elle avait effectué son voyage avait communiqué son itinéraire à son employeur. Son employeur, un ministre du gouvernement fédéral, menait une enquête qui portait sur l'utilisation du congé de maladie du plaignant. Le ministère a demandé au transporteur aérien de confirmer certains renseignements sur l'itinéraire de son voyage.

Le transporteur aérien a hésité. Invoquant ses obligations en vertu de la *LPRPDL*, il a demandé au ministère une preuve attestant que le plaignant avait donné son consentement à une telle communication. Si cela n'était pas possible, le transporteur aérien a suggéré qu'une exemption ou une exception spécifique en vertu de la *Loi* serait nécessaire pour lui permettre de satisfaire à la demande.

En réponse à cette suggestion, le ministère a invoqué une directive en vertu du pouvoir conféré par une loi fédérale particulière, indiquant que les renseignements étaient nécessaires aux fins de l'administration de la loi régissant l'emploi des fonctionnaires fédéraux et a demandé au transporteur

Un FAI tient en « otage » des messages électroniques

Une cliente s'est plainte lorsqu'elle a appris que son fournisseur d'accès Internet (FAI) continuait à recevoir et à stocker ses messages électroniques même si son compte était suspendu. Il s'agit là en réalité d'une pratique normale de l'industrie. Plusieurs FAI utilisent la réception et le stockage continus de messages électroniques comme un moyen pour aller chercher des paiements en retard.

Dans ce cas, l'ancien commissaire a déterminé que le FAI n'avait pas informé la plaignante de manière appropriée des fins liées à l'utilisation des renseignements personnels au cours de la suspension du compte et avait par conséquent utilisé ses renseignements personnels sans son consentement éclairé à des fins autres que celles pour lesquelles les renseignements avaient été recueillis. Compte tenu de ce fait, nous avons conclu que la plainte était fondée.

Mais ce cas a suscité une grande préoccupation pour le Commissariat au sujet de la pratique en question, que nous savions largement répandue dans l'industrie. Dans la lettre de conclusions, l'ancien commissaire a émis le

commentaire suivant :

« ... en tant que commissaire à la protection de la vie privée, je demeure préoccupé au sujet des conséquences que peut avoir la pratique qui consiste à stocker et à conserver des messages potentiellement importants sans informer le destinataire prévu ni de leur existence ni l'expéditeur de leur défaut de livraison. Étant moi-même un utilisateur occasionnel des messages électroniques, au lieu de me laisser croire faussement que le message est passé sans obstacle, j'aimerais bien mieux que le message me soit retourné avec un avis indiquant qu'il n'a pas pu être livré, pour que je puisse ainsi rejoindre le destinataire prévu par d'autres moyens. En réalité, le fait de retourner le message accompagné d'un avis me semble la mesure la plus appropriée et la plus responsable à prendre de telles circonstances pour un fournisseur d'accès Internet. » [traduction]

Néanmoins, la banque dans le deuxième cas était prête à améliorer davantage ses pratiques concernant l'enregistrement des appels téléphoniques. En réponse à cela, le Commissariat a élaboré des lignes directrices sur les « pratiques exemplaires » pour l'enregistrement des appels téléphoniques des clients. En substance, ces lignes directrices soulignent le fait que l'enregistrement des appels téléphoniques implique la collecte de renseignements personnels – une pratique qui devrait respecter les principes équitables de traitement de l'information. En d'autres termes, les conversations ne doivent pas être enregistrées à moins que l'enregistrement ne serve à des fins que toute personne raisonnable considérerait appropriées dans les circonstances. Le client doit être informé de la fin pour laquelle l'appel est enregistré et y consentir, sauf dans un nombre restreint de cas où le consentement n'est pas exigé, et ce avant que l'enregistrement ne commence. Le client devrait également avoir des solutions de rechange telles que celles qui consistent à ne pas enregistrer l'appel, à visiter un point de vente au détail, à rédiger une lettre ou à effectuer une transaction sur Internet.

Un enregistrement sur bande magnétique saisit plus que les données précises nécessaires au but de l'appel. Il enregistre les commentaires, les accents, les attitudes – des renseignements qui peuvent ne pas être pertinents à la documentation nécessaire. C'est pour ces raisons qu'il est important pour les organisations d'être ouvertes avec les clients, de les informer que leur conversation sera enregistrée, d'expliquer pourquoi elle sera enregistrée et de leur offrir des options s'ils ne souhaitent pas être enregistrés.

Dans les deux cas, nous avons fourni aux banques nos lignes directrices sur les « pratiques exemplaires » et les deux organisations ont entrepris d'apporter des améliorations à leurs pratiques d'enregistrement. Dans le premier cas, la banque informe maintenant les clients au début de l'appel que leur conversation est enregistrée et leurs offrent des solutions de rechange pour communiquer leurs renseignements s'ils ne désirent pas poursuivre leur appel. Dans le deuxième cas, la banque a mis en place un message enregistré pour informer les clients que leur conversation sera enregistrée.

consentement. Cette personne avait engagé des procédures judiciaires en cour contre la banque, qu'il tenait responsable de certains retraits effectués avec sa carte bancaire. Au cours de ce processus, la banque a déposé en preuve l'enregistrement d'une conversation téléphonique entre lui et un employé de la banque.

La banque a soutenu qu'elle avait obtenu le consentement de la personne pour enregistrer ses appels. Elle a fait référence à une entente signée par le plaignant lorsqu'il a ouvert son compte, laquelle reconnaissait la pratique d'enregistrement des appels téléphoniques par la banque. Le plaignant avait aussi reçu des brochures sur la protection des renseignements personnels (cinq en tout), qui expliquaient les fins pour lesquelles la banque recueillait des renseignements personnels. Cependant, le plaignant n'avait lu aucun des documents qui lui avaient été remis.

Puis, il y avait la conversation entre un employé de la banque et le plaignant (également enregistrée), dans laquelle l'employé expliquait la pratique d'enregistrement des conversations de la banque. Selon le plaignant, le terme « enregistré » ne signifiait pas nécessairement enregistré électroniquement et il a maintenu sa plainte originale.

L'ancien commissaire a déterminé que la banque avait fait un effort raisonnable pour informer le plaignant de sa pratique, ainsi que de l'objectif de cette pratique, et qu'elle avait obtenu son consentement pour enregistrer ses appels en raison de l'entente qu'il avait signée. Par conséquent, nous avons conclu que la banque s'était conformée aux dispositions pertinentes de la Loi.

Il est clair que des organisations comme celle-ci, qui ont fait un effort pour informer leurs clients et obtenir leur consentement, ont une attente raisonnable à l'égard du fait que les clients liront les documents qui ont été portés à leur attention.

... la plupart des gens

souhaiteraient être

informé avant que leur

appel va ou pourrait

être enregistré.

serait enregistré. On ne lui a pas non plus demandé, après qu'il a appris que son appel avait été enregistré, s'il était d'accord.

La banque avait un point de vue intéressant sur la question du consentement dans de cas. Selon elle, une seule des parties avait à consentir à l'enregistrement des appels. La banque exigeait donc de ses agents de service à la clientèle qu'ils signent un document confirmant leur consentement à l'enregistrement de ces appels.

L'objectif de la banque concernant l'enregistrement des appels était lié au fait qu'elle avait besoin d'une confirmation de la demande du client, ainsi qu'une preuve de son consentement aux modalités du produit ou du service. Selon la banque, l'appel enregistré équivalait à un formulaire signé et est utilisé pour la tenue de dossiers.

Nous sommes d'accord sur le fait que l'information échangée au cours de la conversation devrait être enregistrée d'une certaine façon. Cependant, les attentes raisonnables du client devraient également être prises en considération et la plupart des gens souhaiteraient être informés *avant* que leur appel soit ou puisse être enregistré. Dans ce cas, la banque ne répondait pas du tout à ces attentes et n'avait pas obtenu le consentement du père pour enregistrer cet appel, contrevenant ainsi au principe de consentement de la LPPDE.

Dans le cas de l'autre plainte, une personne alléguait que sa banque avait enregistré ses conversations téléphoniques à son insu et sans son

Clients, faites attention! Vos conversations pourraient être enregistrées

L'ancien commissaire a conclu que les banques avaient invoqué de façon appropriée l'alinéa 9 (3)b) pour refuser aux plaignants l'accès à leurs cotes de crédit internes.

En fin de compte, l'ancien commissaire a décidé d'accorder le bénéfice du doute aux banques. Il l'a fait principalement en raison de son devoir d'équilibrer les droits à la vie privée des personnes et les intérêts légitimes des organisations en matière de renseignements. Considérant la faible valeur informative de la cote de crédit en tant que telle et le fait que l'impossibilité d'obtenir des cotes de crédit internes ne portait pas atteinte de façon significative aux droits à la vie privée des Canadiens et des Canadiennes, nous avons jugé qu'il était tout à fait juste, dans de telles circonstances, d'accepter la position des banques.

Cependant, il reste que deux banques avaient fermement exprimé ce qui nous est apparu comme une profonde conviction et une crainte selon lesquelles des modèles d'attribution de cotes de crédit seraient inévitablement révéls et manipulés de manière frauduleuse, si des personnes avaient accès aux cotes de crédit. Quoique cela nous ait semblé improbable, il était indéniable que les banques s'inquiétaient sérieusement de cette possibilité, que nous avons, par ailleurs, été incapables de réfuter.

par toutes les banques, selon laquelle les fournisseurs de crédit concurrents auraient recours, en fait, à de telles tactiques pour « déchiffrer » les modèles des uns des autres dans le souci de bénéficier d'un avantage concurrentiel.

La pratique d'enregistrer des appels téléphoniques des clients – pratiques assez répandues dans plusieurs organisations – a fait l'objet de deux plaintes. Ces cas illustrent deux approches très différentes prises par les organisations pour informer leurs clients de cette pratique et pour obtenir leur consentement. Dans les deux cas, ainsi que dans ceux impliquant le marketing à des fins secondaires, les attentes raisonnables ont joué un rôle important dans les conclusions de l'ancien commissaire.

En réalité, les banques ne craignaient pas le client moyen, mais les fraudeurs qui essaient de « décoder » le modèle interne d'attribution de cote de crédit à des fins néfastes. Selon les banques, les fraudeurs pourraient employer des moyens détournés pour obtenir un certain nombre de cotes de crédit et pourraient extrapoler le modèle à partir de ces cotes. Les fraudeurs peuvent soit travailler pour des fournisseurs de crédit concurrents des banques, qui essaient de bénéficier d'avantages concurrentiels, soit travailler à leur propre compte, essayant d'obtenir du crédit pour eux-mêmes sur de fausses déclarations.

Dans leurs observations, les banques ont présenté au Commissariat une analyse judiciaire des risques de fraude liés à la disponibilité des cotes de crédit. Cette analyse a conclu que si les cotes de crédit étaient immédiatement accessibles, l'intégrité du modèle d'attribution des cotes de crédit d'une banque pourrait être compromise à partir d'un nombre relativement restreint de cotes de crédit calculées grâce au modèle.

Les scénarios de fraude soulignés par les banques nous ont semblé étranges. Cependant, afin d'être équitables, nous avons demandé conseil à un spécialiste dans le domaine des algorithmes. Ce spécialiste a confirmé qu'avec l'accès aux cotes de crédit personnalisées, il serait assurément plus facile de reproduire approximativement le modèle d'attribution de cotes de crédit interne d'une banque.

Nous en doutons encore. Plus particulièrement, nous étions conscients que l'alinéa 9(3)b), qui utilise le mot « révélerait » plutôt que « pourrait révéler », place la barre très haute pour qui voudrait justifier le refus de communiquer des renseignements personnels. En ce qui concerne l'avis du spécialiste en algorithmes, nous étions disposés à admettre qu'il serait techniquement possible de reproduire approximativement un modèle à partir d'un certain nombre de cotes, mais nous n'étions pas persuadés que cela pourrait se produire. Les observations présentées par les banques ne nous ont pas convaincus que des fraudeurs iraient vraiment jusqu'à agir de la façon décrite dans l'analyse du risque dans le seul but de tromper une banque. Nous étions particulièrement sceptiques à l'égard de la crainte, de toute évidence partagée

En invoquant le paragraphe 9(3)(b), les banques en question ne suggéraient pas qu'une cote de crédit calculée au niveau interne constituait en elle-même des renseignements commerciaux confidentiels, mais plutôt que le modèle utilisé pour calculer une telle cote constituait des renseignements commerciaux confidentiels. Par conséquent, disaient-elles en fait, si les cotes de crédit internes étaient rendues disponibles aux personnes, cela aurait pour effet de faire connaître le modèle avec lequel les cotes sont calculées.

Le problème particulier qu'ils ont soulevé était que les cotes de crédit demandées par les plaignants n'étaient pas les cotes de crédit habituelles fournies par les agences d'évaluation de solvabilité.

Nous avons accepté les arguments des banques selon lesquels le modèle interne d'évaluation de solvabilité représentait un renseignement commercial confidentiel. Mais nous étions beaucoup moins persuadé par l'affirmation plus décisive selon laquelle le fait de communiquer les cotes de crédit pourrait révéler de quelque façon le modèle d'attribution de la cote de crédit lui-même. Comment le simple fait de communiquer à une personne sa cote de crédit pourrait vraisemblablement l'amener à connaître le fonctionnement restreint d'une telle approche logarithmique, technique et compliquée comme le modèle d'attribution d'une cote de crédit?

solvabilité. Dans certains cas, l'institution demandera également une cote de crédit pour le demandeur. Les agences d'évaluation de solvabilité ne calculent pas elles-mêmes les cotes de crédit, mais fournissent plutôt des cotes calculées par une autre entreprise à partir des renseignements détenus par l'agence.

Jusqu'à un certain point, les plaignants avaient de bonnes raisons pour maintenir une telle position. Dans des cas antérieurs, nous avions déjà examiné la question d'accès aux renseignements personnels sur la solvabilité, du moins dans les où des agences d'évaluation de solvabilité étaient impliquées. Nous avions déjà conclu que les cotes de crédit constituent des renseignements personnels selon la définition de la *Loi* et que les personnes ont le droit, en principe, d'y avoir accès. Nous avons déterminé que les agences d'évaluation de solvabilité en particulier doivent se conformer au principe 4.9 de la *Loi* en donnant aux personnes, lorsqu'elles le demandent, accès aux renseignements personnels les concernant contenus dans leur dossier de solvabilité. De plus, nous avons déterminé que les banques, si elles ont obtenues les antécédents de solvabilité d'une personne par une agence d'évaluation de crédit, devaient, dans le même ordre d'idées, donner à la personne accès aux renseignements lorsque celle-ci en fait la demande, y compris la cote de crédit calculée par l'agence.

Mais les cas les plus récents n'étaient pas aussi explicites. Le problème particulier qu'ils ont soulevé était que les cotes de crédit demandées par les plaignants n'étaient pas les cotes de crédit habituelles fournies par les agences d'évaluation de solvabilité. Il s'agissait, en réalité, de cotes de crédit que les banques elles-mêmes avaient calculées et attribuées au niveau interne.

Le fait que les banques aussi possèdent leurs propres cotes de crédit, distinctes de celles fournies par les agences d'évaluation de solvabilité, est généralement moins connu. Les banques calculent leurs propres cotes de crédit internes grâce à leurs propres modèles d'attribution de cote de crédit internes, très différents de ceux qui sont associés aux agences. Tandis que les cotes des agences sont calculées au moyen de modèles standardisés basés presque exclusivement sur les renseignements de solvabilité, une banque élabore des modèles personnalisés tout particuliers, propres à elle et incorporant non

Au cours d'enquêtes sur les plaintes concernant l'évaluation de solvabilité et l'attribution de cotes de crédit, nous avons beaucoup appris sur le fonctionnement de l'industrie d'octroi de crédit en général.

renseignements commerciaux confidentiels ».

Les requérants, croyant au contraire que les cotes de crédit constituaient des renseignements personnels auxquels ils avaient pleinement le droit d'avoir accès, ont porté plainte au Commissariat. Notre tâche principale, dans chacun des cas, consistait à déterminer si l'exemption citée par la banque était valide. Une cote de crédit correspond à une indication numérique de la capacité financière, calculée grâce à un modèle algorithmique. Pour la plupart des gens qui connaissent bien cette notion, le terme « cote de crédit » évoque généralement les agences d'évaluation de solvabilité. Ces agences offrent aux banques et aux autres institutions d'octroi de crédit des services de renseignements sur les antécédents en matière de solvabilité de clients potentiels, y compris parfois les cotes de crédit. En examinant une demande de crédit, une institution d'octroi de crédit obtiendra souvent les antécédents en matière de solvabilité du demandeur par une agence d'évaluation de

Dans deux cas particuliers, les personnes avaient fait des demandes officielles en vertu de la LPRPDE afin d'avoir accès à certains renseignements personnels contenus dans des dossiers détenus par leurs banques. Plus particulièrement, chaque requérant voulait connaître sa cote de crédit. Les banques en question leur en ont refusé l'accès, invoquant la disposition d'exemption stipulée au paragraphe 9(3)(b) de la Loi. Cette disposition stipule, de fait, qu'une organisation n'est pas tenue de communiquer à l'intéressé des renseignements personnels, dans le cas où la communication « révélerait des

public normal », comparable à des « potins anodins ». La banque a même suggéré qu'elle avait le droit de communiquer de tels renseignements dans un souci de « courtoisie commerciale » et de protection de ses propres intérêts. En citant le paragraphe 5(3) et le principe 4.3.5, les soi-disantes dispositions relatives à la « raisonnable » de la LPRPD, la banque a également suggéré que le plaignant n'avait aucune attente raisonnable en matière de protection de la vie privée et que des personnes raisonnables auraient considéré la communication appropriée dans les circonstances.

Bien que nous n'ayons pas été rébarbatifs face à la banque et que nous ayons été prêts à concéder jusqu'à un certain point le caractère raisonnable du point de vue de la banque, l'ancien commissaire devait établir la distinction de quelque part. En présentant ses conclusions au plaignant, il a formulé le commentaire suivant :

« À mon avis,.... le caractère raisonnable de la situation s'arrête exactement au point où le directeur [de la banque], sachant que vous aviez agi en votre propre nom à sa succursale ce matin-là, a néanmoins pris le téléphone à son bureau pendant les heures de travail pour informer votre employeur. Ce n'était pas une communication anodine ou par inadvertance. Ce n'était pas des potins anodins. Il s'agissait d'un acte délibéré de communication de renseignements personnels à un tiers par une personne agissant en sa qualité officielle, qui n'était nullement habilitée à faire cette communication. En outre, la Loi place les droits des personnes au-dessus de notions comme la « courtoisie commerciale » et ne fait pas de distinction quant à la taille de la localité qu'habite la personne. Y a-t-il quelque part une personne raisonnable qui s'attendrait à ce que son directeur de banque communique à son employeur des renseignements concernant ses affaires bancaires personnelles? La réponse à cette question est évidemment non. » [traduction]

Une fraude relative à la cote de crédit

Au cours d'enquêtes sur les plaintes concernant l'évaluation de solvabilité et l'attribution de cotes de crédit, nous avons beaucoup appris sur le fonctionnement de l'industrie d'octroi de crédit en général.

Après avoir reçu la lettre de conclusion, la compagnie de transport aérien a accepté la recommandation de l'ancien commissaire et pris des dispositions pour offrir la formation à un autre endroit au pilote et aux autres personnes qui refusaient de signer le formulaire.

Communication inappropriée, par une banque, de renseignements personnels à l'employeur de l'intéressé

Une personne s'est présentée à sa banque pour une affaire personnelle : contester les frais pour des chèques. Il n'était pas satisfait de la réponse de la banque et une dispute a eu lieu.

Le directeur de la succursale est entré en scène et a décidé que son personnel n'avait plus à composer avec le client. Il s'est trouvé que l'entreprise qui employait le client faisait d'importantes affaires avec la banque. Avant de mettre fin à la relation entre la banque et le client, le directeur de la succursale a jugé bon de discuter de cette question avec l'employeur du client.

Le plaignant était surpris lorsque son employeur l'a confronté au sujet de ce qui s'était passé plus tôt ce matin-là à la banque.

L'une de nos premières tâches dans cette enquête était de déterminer exactement ce qui avait été communiqué par téléphone entre le directeur de la banque et l'employeur. Puisque rien ne prouvait qu'ils avaient discuté des affaires financières du plaignant, il semblait que la communication effective avait été limitée à trois simples faits : (1) que le plaignant avait un compte à cette succursale ; (2) que son compte serait bientôt fermé ; (3) qu'il y avait eu une scène avec le caissier ou la caissière.

Selon la banque, rien de cela ne peut être considéré comme étant des renseignements personnels concernant le plaignant. La banque a souligné que la scène, elle-même, s'était produite dans un endroit public et dans une petite communauté, à un endroit où le fait d'effectuer des opérations bancaires est difficilement affaire de secret. La position prise par la banque était que la communication en question entrerait dans la catégorie du « discours

Pour parvenir à cette décision, nous nous sommes fîs au « critère de la personne raisonnable » énoncé au paragraphe 5(3) de la *LPDP* afin d'évaluer les buts de la compagnie de transport aérien. Nous avons reconnu que les motifs de la compagnie exigeant que ses pilotes signent un tel formulaire semblaient raisonnables à première vue. Toutefois, au-delà des apparences, les motifs cessent d'être acceptables. Nous avons estimé qu'il n'était pas vraiment à l'honneur de la compagnie de transport aérien de faire passer le coût et la commodité avant le droit du pilote de refuser de consentir à des pratiques de collecte et de communication qui contrevenaient manifestement à la loi canadienne. Nous avons fait remarquer que la compagnie de transport aérien avait des options, mais avait choisi de ne pas s'en prévaloir.

En déterminant que les motifs de la compagnie de transport aérien ne se conformaient pas aux exigences du paragraphe 5(3), l'ancien commissaire a émis, dans sa lettre de conclusion, le commentaire suivant sur cet exemple opportun concernant la difficulté à tenir l'équilibre entre les exigences en matière de sécurité et le droit fondamental à la vie privée :

« Je conviens que les circonstances dans lesquelles se trouvent de nombreux pays, tout particulièrement les États-Unis, justifient la prise de certaines mesures de sécurité. Naturellement, il est raisonnable d'exiger que les pilotes reçoivent une autorisation de sécurité afin de pouvoir voler et c'est la raison pour laquelle le Canada a établi des mesures de sécurité auxquelles sont assujettis les pilotes de compagnies aériennes commerciales au Canada... Mais est-ce qu'une personne raisonnable trouverait qu'il est approprié d'exiger que ces mêmes pilotes consentent à des pratiques inacceptables de collecte et de communication de renseignements personnels à la demande d'un gouvernement étranger? Je ne le crois pas. En fait, je soupçonne que la plupart des Canadiens et Canadiennes trouveraient que cet empiètement sur les droits canadiens est hautement inadmissible et exigerait que le l'employeur offre des options raisonnables aux employés et que le gouvernement souleve la question avec les États-Unis. » [traduction]

gouvernement canadien, la compagnie de transport aérien, le syndicat – mais il n'y avait aucune solution immédiate à l'horizon. Le gouvernement fédéral avait demandé aux États-Unis d'accepter la vérification, faite au Canada, des antécédents des pilotes de compagnies aériennes commerciales. Mais, au moment de la plainte, les États-Unis n'avaient pas encore pris de décision.

La compagnie de transport aérien était troublée par le libellé du formulaire, mais se trouvait dans une situation difficile. La loi exige que ses pilotes soient formés. L'autre école de pilotage la plus proche se trouvait en Europe – ce qui aurait été plus coûteux que d'envoyer ses pilotes en Floride. De plus, étant donné que le pilote et le copilote doivent recevoir la formation en même temps, la compagnie de transport aérien se trouverait dans une position délicate si un pilote était disposé à signer le formulaire tandis que l'autre ne l'était pas.

Le syndicat des pilotes a protesté contre l'exigence de signer le formulaire. Il a négocié une entente avec la compagnie de transport aérien qui stipule, entre autres, que la décision de signer le formulaire était volontaire et que la compagnie offrirait une formation de rechange aux pilotes qui s'y opposaient. Le pilote a décidé de ne pas signer le formulaire. Bien que son employeur ait obtenu une prorogation temporaire de son permis jusqu'à ce qu'une solution puisse être trouvée, il n'a pris aucune autre disposition en vue d'une formation pour lui. À moins que le gouvernement américain n'accepte la demande du Canada ou que l'ancien commissaire à la protection de la vie privée ne rende ses conclusions, la compagnie de transport aérien refuserait de modifier sa décision. La prorogation du permis du pilote est finalement venue à échéance.

Nous nous sommes vivement opposés au formulaire d'autorisation. Nous l'avons trouvé tout à fait inadmissible à de nombreux égards et nous avons conclu que les pratiques qu'il autorisait ne respectaient pas du tout les principes équitables en matière de traitement de l'information, qui sont la pierre angulaire des lois sur la protection des renseignements personnels au Canada.

Des pilotes canadiens affectés par des mesures de sécurité prises par les États-Unis

Les Canadiennes et Canadiens moyens continuent de ressentir les contre-coups des événements du 11 septembre 2001. Une personne directement touchée par les nouvelles mesures de sécurité, un pilote d'une compagnie aérienne commerciale, s'est vu confronté à un choix difficile : renoncer à ses droits à la vie privée ou risquer de perdre son emploi. Dans le passé, lorsque le pilote devait suivre une formation de pilotage requise pour maintenir son permis, son employeur l'inscrivait simplement à une école de pilotage en Floride. Cette procédure a changé après le 11 septembre 2001. Les écoles de pilotage américaines sont à présent tenues de faire signer un formulaire d'autorisation par leurs étudiants étrangers, y compris les pilotes canadiens de compagnies aériennes commerciales. Ce formulaire permettrait au gouvernement des États-Unis de recueillir et de communiquer des renseignements personnels concernant les étudiants. Toutefois, il n'a pas

adéquatement expliqué les raisons de cette collecte et communication, ni n'a semble établir des limites à cet égard.

Lorsque son employeur lui a demandé de signer le formulaire, le pilote était outré. Après tout, le gouvernement canadien avait déjà fait une vérification approfondie de ses antécédents. Il n'aimait pas l'idée d'un gouvernement étranger passant au crible ses antécédents, d'autant plus qu'il ne savait pas clairement quels renseignements seraient recueillis et à qui ils seraient communiqués.

Personne ne semblait à l'aise relativement au formulaire – le

Il n'aimait pas l'idée d'un gouvernement étranger passant au crible ses antécédents, d'autant plus qu'il ne savait pas clairement quels renseignements seraient recueillis et à qui ils seraient communiqués.

L'ancien commissaire a déterminé que cette plainte était fondée.

[traduction] « pour vous. »

réduire la possibilité d'une mauvaise décision aux conséquences défavorables aurait dû prendre soin de veiller à l'exacitude de ces renseignements afin de renseignements personnels pour vous soupçonner d'un crime, [la banque] pain. Sachant bien que la police se servirait probablement de vos de l'embaras et des inquiétudes à propos de votre réputation et de votre gagne-crime. Qui plus est, ce fut une décision qui vous a causé une triste réputation, erronée selon laquelle vous étiez recherchée en tant que suspecte principale d'un ont servi à prendre une décision à votre sujet – en particulier, une décision renseignements personnels communiqués de façon inappropriée par [la banque] possibles de renseignements inexacts sur une personne. J'ai déterminé que vos « ...une organisation doit bien tenir compte des conséquences néfastes

de conclusion adressée à la plaignante, l'ancien commissaire a écrit :
conséquent, elle a clairement enfreint le principe 4.6 de la Loi. Dans sa lettre communiquée était aussi exacte que possible. Elle ne l'a pas fait et, par Pour cette raison seulement, la banque aurait dû s'assurer que l'information situation où l'exacitude avait été décisive dans le but de résoudre un crime. photographie de la plaignante – étaient entièrement inexacts dans une Nous avons déterminé que les renseignements personnels en question – la renseignements personnels.

qu'a la banque, en vertu de la LPRPDE, d'assurer l'exacitude des commissaire, nous avons examiné la question en fonction des obligations En ce qui concerne la résolution de sa plainte officielle adressée à l'ancien que dans un seul article de journal.

Commissariat a pu rassurer la plaignante que sa photographie n'avait paru fait que son image avait peut-être paru dans d'autres avis d'Échec au crime. Le

Toutefois, la plaignante n'était pas entièrement satisfaite. Après le choc initial et le bouleversement, elle est devenue bien plus préoccupée par l'effet qu'avait l'incident sur sa réputation, lorsqu'elle a appris que de nombreuses personnes l'avaient bel et bien reconnue dans l'article. Cela était tout particulièrement inquiétant, parce que son travail dépendait de sa capacité de se rendre aux résidences et aux lieux de travail de ses clients. Elle était aussi préoccupée du

pour vérifier les heures des bandes vidéo de surveillance et des bandes journal. semblables. La banque a aussi mis en œuvre des changements de procédure collaboré à l'élaboration de mesures visant à prévenir des situations procédures normales de vérification dans ce cas et tous deux ont depuis police et *Échec au crime* ont tous deux admis par la suite ne pas avoir suivi les a reçu des excuses officielles de la banque, de la police et d'*Échec au crime*. La plaignante avait été la victime d'une erreur sur la personne. La plaignante même jour, le journal a publié, en page de couverture, un article précisant que corrigé l'erreur en publiant une rétractation dans le même quotidien. Le Une semaine après l'article « Crime de la semaine » initial, *Échec au crime* a

Échec au crime, illustraient la mauvaise personne.

son tour donné à l'organisme police local, et que la police a à remises par la suite au service de Ainsi, les photos que la banque a

c'est-à-dire la plaignante.

quelque 12 minutes plus tôt, chèques au guichet de la caissière personne qui avait encaissé les chèques. C'était plutôt celle de la femme qui avait précédé la vraie personne qui avait encaissé apparaissait n'était pas celle de la bande journal, l'image qui l'encaissement indiquée par la bande vidéo jusqu'à l'heure de

À sa grande horreur, la plaignante a vu sa propre image dans une photographie accompagnant l'article « Crime de la semaine » d'Échec au crime.

Résolue : Cela signifie que l'organisation a pris des mesures correctives pour remédier à la situation, ou que le plaignant est satisfait des résultats de l'enquête menée par le Commissariat à la protection de la vie privée du Canada.

Abandonnée : Il s'agit d'une enquête qui a pris fin avant que toutes les allégations n'aient été pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons, par exemple, lorsque le plaignant n'est plus intéressé à donner suite à l'affaire.

SOMMAIRE DE CAS CHOISIS EN VERTU DE LA LPPDE Cas portant sur une erreur sur la personne

Une plaignante a écrit au Commissariat pour signaler qu'un ami l'avait informé d'un avis paru dans le journal selon lequel elle était recherchée par la police. À sa grande horreur, la plaignante a vu sa propre image dans une photographie accompagnant l'article « Crime de la semaine » d'*Échéec au crime*. L'article faisait état d'un récent vol de deux chèques d'une femme âgée et désignait la personne illustrée comme suspecte du crime. L'image avait été saisie par une caméra de surveillance vidéo à la banque. La caméra était braquée sur le guichet de la caissière où le voleur avait encaissé les chèques volés.

Il s'est avéré que la plaignante s'était en effet présentée à la même banque et au même guichet le jour en question, mais non pas pour encaisser un chèque. Elle y était allée simplement pour régler une facture. Il était clair qu'elle n'était pas l'auteur du crime.

Comme notre enquêteur l'a appris, il s'agissait de la même banque, du même guichet, du même jour, mais non de la même heure.

Le jour en question, l'horloge de la bande journal de la banque (son registre central informatisé de toutes les transactions) avait 12 minutes de retard sur l'horloge de la caméra vidéo. Lorsque le personnel de sécurité a fait avancer la

plaintes, 16 %, avait été déposé à l'endroit d'autres types d'organisations, dont les fournisseurs d'accès Internet, les agences d'évaluation du crédit et les conseils de bandes autochtones.

En 2002, l'ancien commissaire a rendu des conclusions sur 162 plaintes déposées en vertu de la *LPRPDE*, comme suit :

Non fondées	61
Fondées	45
Résolues	41
Abandonnées	15

De plus, le Commissariat a aussi mené cinq enquêtes sur des incidents. Les incidents sont des questions provenant de diverses sources, notamment les médias, dont le commissaire prend connaissance. Habituellement dans pareil cas, la victime n'est pas nommée et le Commissariat n'a reçu aucune plainte.

Ce qui suit dans ce rapport constitue des exemples des cas les plus notables de l'année. Des résumés plus détaillés de toutes les conclusions en vertu de la *LPRPDE* se trouvent sur notre site Web à l'adresse www.privcom.gc.ca. Ces conclusions sont affichées dans le but de donner une orientation aux organisations et à la collectivité juridique sur l'application de la Loi.

DÉFINITION DE CONCLUSIONS EN VERTU DE LA *LPRPDE*

Non fondée : Cela signifie qu'il n'y a pas de preuve qui porte le commissaire à la protection de la vie privée à conclure que l'organisation a enfreint la Loi sur la protection des renseignements personnels et les documents électroniques (*LPRPDE*).

Fondée : Cela signifie que l'enquête a révélé que l'organisation n'a pas respecté une des dispositions de la Loi sur la protection des renseignements personnels et les documents électroniques (*LPRPDE*).

Au cours de l'année civile 2002, le Commissariat a reçu 300 plaintes en vertu de la *LPRPDE* de personnes alléguant que leurs droits à la vie privée avaient été enfreints par toute une gamme d'organisations. Environ 37 % des cas portaient sur des pratiques du secteur bancaire, suivis de 19 % dans les secteurs des télécommunications et la radiodiffusion, 15 % dans les entreprises de transport et 13 % dans le secteur nucléaire. Le reste des

ENQUÊTES ET DEMANDES DE RENSEIGNEMENTS

En vertu de la *LPRPDE*, le commissaire est tenu de soumettre un rapport annuel au Parlement sur les activités du Commissariat au cours de l'exercice antérieur. En ce qui concerne la *LPRPDE*, le présent rapport porte sur la période du 1^{er} janvier 2002 au 31 décembre 2002.

Nous avons aussi entrepris un certain nombre d'activités de communication en vue d'une sensibilisation sur les questions liées au droit à la vie privée et sur les lois fédérales concernant la protection des renseignements personnels. Du 1^{er} avril 2002 au 31 mars 2003, l'ancien commissaire et les cadres supérieurs ont prononcé 49 allocutions lors de conférences et événements spéciaux ; nous avons émis plus de 25 communiqués et avis aux médias sur des questions-clé touchant au droit à la vie privée ; nous avons répondu à des centaines de demandes de renseignements et d'entrevues adressées par les médias ; nous avons distribué plus de 23 000 exemplaires de nos publications à des particuliers, à des entreprises et autres organisations à travers le pays ; et nous avons reçu un nombre plus croissant que jamais de visites sur notre site web, soit en moyenne 50 000 visites par mois.

La deuxième année complète d'application de la *LPRPDE* s'est avérée à la fois intéressante et stimulante pour le Commissariat à plusieurs égards. Nous avons commencé à recevoir des plaintes concernant les renseignements personnels sur la santé des personnes et à faire enquête sur ces plaintes. Nous avons aussi fait des percées importantes sur une kyrielle de questions, dont le consentement et le marketing, la cote de solvabilité, l'enregistrement des appels téléphoniques et les autorisations de sécurité.

Partie II

Rapport concernant la Loi sur la protection des renseignements personnels et les documents électroniques

INTRODUCTION

La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) établit des règles de base sur la façon dont les organisations du secteur privé peuvent recueillir, utiliser et communiquer des renseignements personnels dans le cadre de leurs activités commerciales.

Depuis l'entrée en vigueur de la Loi, le 1^{er} janvier 2001, elle s'est principalement appliquée aux activités commerciales de ce qu'on appelle les installations, les ouvrages, les entreprises ou les secteurs d'activité fédéraux, notamment les entreprises de transport et de télécommunications, les banques et les radiodiffuseurs. Elle s'applique aussi aux renseignements personnels des employés de ces entreprises, ainsi qu'à la vente, à la location ou au troc de renseignements personnels au-delà des frontières provinciales ou nationales par des organisations sous réglementation provinciale. Depuis le 1^{er} janvier 2002, les renseignements personnels sur la santé recueillis, utilisés ou communiqués par ces organisations sont aussi couverts. À compter du 1^{er} janvier 2004, la LPRPDE portera également sur la collecte, l'utilisation ou la communication de renseignements personnels dans le cadre de toutes les activités commerciales au Canada, sauf dans les provinces qui auront adopté une loi jugée essentiellement similaire à la loi fédérale.

Commissaire à l'information du Canada c. Commissaire de la GRC et autre

Numéro du greffe 28601 de la Cour suprême du Canada

Une liste des affectations de quatre agents de la Gendarmerie royale du Canada (GRC) avait fait l'objet d'une demande aux termes de la *Loi sur l'accès à l'information*. Le commissaire de la GRC a refusé de communiquer les renseignements parce qu'ils se rapportaient aux antécédents professionnels de ces personnes et qu'il s'agissait ainsi de renseignements personnels aux termes de l'article 3 de la *Loi sur la protection des renseignements personnels*. Le commissaire à l'information a soutenu toutefois que l'alinéa 3 j) portant sur la définition de renseignements personnels dans la *Loi sur la protection des renseignements personnels* stipule que les renseignements relatifs aux postes ou fonctions d'agents ou de fonctionnaires du gouvernement ne constituent pas des renseignements personnels pour l'application de l'article 19 de la *Loi sur l'accès à l'information*.

État de la situation

Le 6 mars 2003, la Cour suprême du Canada a fait part de sa décision unanime. La Cour a très clairement déclaré que l'information peut être personnelle et néanmoins être visée par la rubrique de l'alinéa 3 j) qui précise les caractéristiques générales associées au poste ou fonctions d'un agent ou d'un fonctionnaire d'une institution fédérale. La Cour suprême a estimé qu'aucun des renseignements demandés ne concernait la compétence ou les caractéristiques des employés. Par conséquent, elle a ordonné que les renseignements suivants soient communiqués pour chacune des personnes nommées : une liste des affectations antérieures, avec statut et dates, une liste des grades et les dates auxquelles ces grades ont été obtenus, ainsi que les années de service et la date d'anniversaire du service.

La décision de la Cour suprême restreint l'application de l'alinéa 3 j) relatif à la définition de renseignements personnels. Bien que le Commissariat ait plaidé en faveur d'une interprétation plus restreinte de l'exception, la décision de la Cour suprême n'est pas sans fondement.

La GRC a informé le Commissariat qu'elle avait mis fin, le 28 août 2001, à l'enregistrement vidéo continu par caméra de surveillance que si une il n'y aurait enregistré vidéo du secteur sous surveillance que si une infraction à la loi était constatée. Bien que cela assure la conformité de l'utilisation de la caméra de surveillance vidéo avec la lettre de la *Loi sur la protection des renseignements personnels*, qui ne s'applique techniquement qu'aux renseignements « quels que soient leur forme et leur support », l'ancien commissaire était d'avis que la poursuite de la surveillance par caméra vidéo même en l'absence d'enregistrement continu ne respecte pas suffisamment l'esprit de la *Loi sur la protection des renseignements personnels* et de la protection des droits à la vie privée des Canadiens et Canadiennes.

Le 21 juin 2002, l'ancien commissaire a déposé une déclaration à la Cour suprême de la Colombie-Britannique, pour demander que la Cour déclare que cette surveillance vidéo généralisée était inconstitutionnelle, enfreint la *Charte*, ainsi que les obligations internationales du Canada en matière de droits de la personne. Du 12 au 14 mars 2003, une audience a été tenue concernant la requête du gouvernement fédéral demandant à la cour de rejeter la cause. La cour a statué que le commissaire n'était pas légalement habilité à tenter une action en justice.

État de la situation

Le 4 juillet 2003, le commissaire nouvellement nommé a annoncé que le Commissariat avait demandé à l'avocat de retirer son appel relatif à l'affaire. Bien que le commissaire et le Commissariat aient toujours diverses préoccupations en ce qui a trait à la surveillance vidéo des endroits publics par des autorités publiques, le fait de poursuivre cette action particulière n'était pas perçu comme un moyen efficace de dépenser les fonds publics.

renseignements personnels. Tout d'abord, la Société canadienne des postes a enfreint le paragraphe 5(2) de la Loi en omettant d'informer les abonnés au service du PNCA de son intention de communiquer leurs nouvelles adresses à des expéditeurs de courrier grand public et des entreprises de marketing direct à des fins commerciales. Puis, elle a enfreint l'article 8 en omettant d'obtenir le consentement des personnes en vue de la communication de leurs nouvelles adresses aux expéditeurs de courrier grand public et aux entreprises de marketing direct.

État de la situation

Le 13 février 2002, la Société canadienne des postes a introduit une requête alléguant que l'ancien commissaire avait outrepassé ses compétences dans son application des articles 5 et 8 de la Loi sur la protection des renseignements personnels. Toutefois, le 4 avril 2002, la Société canadienne des postes a convenu d'ajouter une case à cocher sur son formulaire, qui permet aux personnes de consentir à cette activité. La question a donc perdu sa raison d'être et la Société canadienne des postes a abandonné sa requête le 14 avril 2002.

Commissaire à la protection de la vie privée c. procureur général du Canada et autre

Numéro du greffe S57566 de la Cour suprême de la Colombie-Britannique

Le Commissariat a reçu, en juin 2001, une plainte concernant l'installation de caméras de surveillance vidéo par la Gendarmerie royale du Canada (GRC) au centre-ville de Kelowna, C.-B. À la suite d'une enquête, l'ancien commissaire a déterminé que, par l'enregistrement continu plutôt que l'enregistrement de certains incidents liés à des activités d'application de la loi, la GRC recueillait inutilement des renseignements sur des milliers de citoyens innocents se livrant à des activités qui n'avaient nullement rapport avec le mandat de la GRC. Par conséquent, il a conclu que la surveillance vidéo à Kelowna enfreignait la Loi sur la protection des renseignements personnels.



Toutefois, il prend également part à des litiges en dehors de l'application de la Loi sur la protection des renseignements personnels. Voici un résumé des litiges concernant d'importantes questions relatives au droit à la vie privée auxquels le commissaire a pris part.

Mertie Anne Beatty et autre c. Statisticien en chef et autre

Numéro du greffe T-178-02 de la Cour fédérale du Canada

Cette question a été portée devant la Cour fédérale du Canada par un groupe de citoyens canadiens qui ont demandé l'accès aux relevés du recensement de 1906 pour les provinces du Manitoba, de la Saskatchewan et de l'Alberta conformément à l'article 6 du *Règlement sur la protection des renseignements personnels*.

La position du Commissariat a toujours été que la communication des renseignements recueillis lors du recensement de 1906 est interdite par les dispositions en matière de confidentialité de la Loi sur la statistique et qu'on devrait, par conséquent, envisager des modifications à la Loi comme voie de compromis.

État de la situation

La requête a été déposée en février 2002. Après avoir examiné la loi, le gouvernement fédéral a décidé que l'information pouvait, en fait, être communiquée et fit ainsi. Le projet de loi S-13 a été présenté par la suite dans le but de modifier rétroactivement les lois sur le recensement afin de permettre l'accès aux dossiers et répondre aux préoccupations en matière de protection des renseignements personnels. En conséquence de quoi, la requête a été abandonnée.

Société canadienne des postes c. Commissaire à la protection de la vie privée

Numéro du greffe T-233-02 de la Cour fédérale du Canada

Le 14 janvier 2002, l'ancien commissaire a déterminé que le service du Programme national sur les changements d'adresse (PNCA) de la Société canadienne des postes enfreignait à deux égards la Loi sur la protection des

Une des leçons à tirer de notre expérience des onze derniers mois est le besoin d'une meilleure formation sur le fonctionnement de l'ÉFVP comme mécanisme de gestion des risques. Une autre concerne la nécessité pour les ministères d'informer et de faire participer le Commissariat le plus tôt possible à l'élaboration de l'ÉFVP.

Étant donné le besoin qu'ont les organisations d'une meilleure compréhension de la politique sur l'ÉFVP, nous conseillons aux représentants du gouvernement de communiquer avec le Secrétariat du Conseil du Trésor ou de consulter son site Web à l'adresse www.tbs-sct.gc.ca, afin d'obtenir de plus amples informations.

DEVANT LES TRIBUNAUX

Aux termes de l'article 41 de la *Loi sur la protection des renseignements personnels*, une personne est autorisée, à l'issue d'une enquête par le Commissaire, à déposer auprès de la Cour fédérale du Canada un recours en révision d'une décision d'une institution fédérale qui lui a refusé l'accès à ses renseignements personnels. Depuis l'entrée en vigueur de la *Loi sur la protection des renseignements personnels* en 1983 jusqu'au 31 mars 2003, environ 130 recours en révision ont été déposés auprès de la Cour fédérale. Huit ont été déposés au cours de l'exercice qui a pris fin le 31 mars 2003.

L'article 42 de la *Loi sur la protection des renseignements personnels* autorise le commissaire à comparaître devant la Cour fédérale. Le commissaire peut exercer lui-même un recours en révision de la décision d'une institution fédérale qui a refusé l'accès à des renseignements personnels, dans la mesure où il obtient le consentement de la personne qui a demandé les renseignements. Il peut également comparaître devant la Cour au nom de la personne qui a exercé le recours devant elle en vertu de l'article 41 ou comparaître, avec l'autorisation de la Cour, comme partie à une instance engagée en vertu de l'article 41.

Il n'y a actuellement aucun recours judiciaire en vertu de la *Loi sur la protection des renseignements personnels* auquel le commissaire participe activement.

- une description adéquate du processus administratif ;
- un organigramme de données ou un organigramme complet ;
- une description adéquate de l'infrastructure pour la sécurité des données associée au projet.

En outre, les documents d'information manquants comprennent souvent les suivants :

- projets d'entente où sont concernés des tiers fournisseurs de services ;
- rapports d'évaluation de la menace et des risques (EMR), le cas échéant ;
- études de faisabilité de projet, le cas échéant ;
- plans de gestion de projet, liés à la conception du projet ;
- spécifications techniques relatives à la conception du système.

Nous avons également observé un certain nombre de problèmes communs en ce qui concerne l'analyse de la protection des renseignements personnels, dont les suivants :

- la confusion de la protection des renseignements personnels avec la sécurité et la confidentialité ;
- le fait de voir le processus d'EFVP essentiellement comme un exercice de vérification de la conformité en matière de protection des renseignements personnels ;
- l'omission d'établir un lien entre les risques déterminés et les éléments particuliers de la conception du projet ;
- des mesures d'atténuation proposées qui ne traitent pas du risque déterminé ;
- des mesures d'atténuation proposées pour des risques non encore déterminés.

Bien que ces problèmes et omissions reflètent le manque de connaissances des ministères à propos de la politique sur l'EFVP, il est à noter que nous commençons maintenant à voir une amélioration générale de la qualité des EFVP que nous recevons.

Le rôle du commissaire

ne consiste pas à

approuver ou à rejeter

les projets évalués dans

le cadre de l'EFVP, mais

plutôt à déterminer si les

ministères ont bien

évalué l'incidence sur le

droit à la vie privée d'un

projet ou d'une

proposition.

de la politique ni aux lignes directrices associées à la politique. Par conséquent, la plupart ont été retournées aux ministères ou retirées par ces derniers pour en faire la révision conformément à la politique. Jusqu'à présent, huit EFVP reçues ont passé toutes les étapes du processus d'examen.

Bien que la majorité des rapports reçus jusqu'à présent des ministères concernent des EFVP, nous avons constaté au cours de l'année une augmentation du nombre d'évaluations préliminaires des facteurs relatifs à la vie privée (EFVP). Nous pensons que cela reflète une tendance de la part des ministères à adopter une approche plus prudente et progressive à l'élaboration de leurs EFVP, compte tenu de leur manque de connaissances à propos du processus et du manque probable de compétences internes à cet égard. Lorsque les ministères doivent respecter une date limite fixe et imminente pour la mise en œuvre, nous leur conseillons de rédiger directement leur EFVP pour accélérer le processus d'examen.

Jusqu'à présent, il n'y a eu aucune EFVP, et certainement aucune EFVP, pour lesquelles le personnel du Commissariat n'a pas jugé nécessaire de s'adresser au ministère concerné pour obtenir des renseignements supplémentaires. Parmi certains des éléments fréquemment omis, mentionnons les suivants :

- un calendrier de mise en œuvre du projet ;
- un inventaire complet des éléments de données recueillis et utilisés (les renseignements peuvent être décrits mais non détaillés) ;

Cinq des 17 EFVP que nous avons reçues ont été rédigées avant l'entrée en vigueur de la politique du SCT et ainsi ne se conformaient ni aux exigences

La plupart de ces initiatives ou projets concernent la prestation électronique de services à des personnes par le biais du réseau Internet, de sorte que les risques en matière de protection des renseignements personnels proviennent de diverses sources, dont les caractéristiques des systèmes, l'infrastructure technique et la conception du service ou du programme électronique.

Dans le but d'assumer cette nouvelle responsabilité, nous avons créé une nouvelle division au sein de la Direction des examens et des pratiques en matière de vie privée, entièrement dédiée à l'analyse et à la présentation de commentaires sur les EFVP qui nous sont soumises pour examen.

Le rôle du commissaire ne consiste pas à approuver ou à rejeter les projets évalués dans le cadre de l'EFVP, mais plutôt à déterminer si les ministères ont bien évalué l'incidence sur le droit à la vie privée d'un projet ou d'une proposition.

de services, nouveaux ou modifiés, qui soulèvent des questions relatives au droit à la vie privée. Les ministères doivent aussi consulter le Commissariat lorsqu'ils préparent une EFVP pour s'assurer d'identifier les risques touchant au droit à la vie privée et pour s'assurer que les mesures d'atténuation prises pour traiter de ces risques sont appropriées. En examinant la documentation de concert avec les représentants des institutions, le Commissariat est donc en mesure de donner des conseils et une orientation à ces institutions et de trouver des solutions aux risques éventuels pour la protection des renseignements personnels.

Les programmes et services actuels et nouveaux qui présentent des risques possibles en matière de vie privée sont à présent assujettis à une EFVP, qui est en fait une étude de faisabilité du point de vue du droit à la vie privée. Elle implique des remaniements importants de programmes actuels lorsque le remaniement porte sur une collecte, une utilisation ou une communication, nouvelle ou accrue, de renseignements personnels, un nouveau couplage de données, l'impartition ou d'autres changements qui risquent de soulever de nouvelles préoccupations relatives au droit à la vie privée.

Une EFVP est conçue pour donner aux ministères et organismes du gouvernement fédéral un cadre uniforme pour prévoir l'incidence d'une proposition sur le droit à la vie privée, évaluer sa conformité avec les lois et les principes sur la protection des renseignements personnels et déterminer quelles mesures d'atténuation sont requises pour surmonter les répercussions néfastes. Une EFVP bien exécutée permet d'éviter des frais supplémentaires, la mauvaise presse, la perte de crédibilité et de confiance du public, qui pourraient découler d'une proposition qui ne tient pas compte du droit à la vie privée. Il s'agit aussi d'une façon d'accroître la sensibilisation et la compréhension au sujet des principes de protection des renseignements personnels, tant de façon interne qu'auprès des citoyens.

La tenue d'une EFVP constitue une responsabilité de gestion partagée. Comme l'énonce la politique du Conseil du Trésor, les EFVP sont des activités de collaboration qui exigent des compétences diverses, notamment celles de gestionnaires de programme, de techniciens spécialisés, de conseillers juridiques et de conseillers en matière de protection des renseignements personnels. Bien qu'il incombent à l'administrateur général d'une institution, d'un ministère ou d'un organisme fédéral de déterminer s'il y a lieu de procéder à une EFVP, plusieurs ministères ont établi des comités internes dans le but d'examiner les projets ministériels pour déterminer si une EFVP est requise ou non. Compte tenu de la nature multidisciplinaire de l'exercice, cela nous semble une mesure sage.

Il est tout particulièrement important de noter que la politique exige que les ministères informant le Commissariat de toute proposition de programmes et

au moyen d'une évaluation des facteurs relatifs à la vie privée (EFVP), qui exige un examen plus rigoureux. Nous abordons de façon plus détaillée les évaluations des facteurs relatifs à la vie privée dans la section suivante de ce rapport.

Nous avons régulièrement remarqué une amélioration dans le détail et l'intégrité des présentations de DRHC à propos des questions relatives aux droits à la vie privée. Dans notre dernier rapport, nous avons exprimé des réserves concernant le fait que DRHC a communiqué des renseignements restreints relativement à des marchés passés avec des parties de l'extérieur et nous avons affirmé que DRHC devrait renforcer l'obligation contractuelle de ces parties afin de protéger le caractère privé des renseignements personnels durant leur administration temporaire. Bien que certaines des présentations que nous avons reçues ne répondent pas pleinement à nos attentes, le Ministère a réalisé des progrès en ce qui concerne ce problème au cours de la dernière année.

ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

Le 2 mai 2002, le Secrétaire du Conseil du Trésor du Canada a rendu publique une nouvelle directive exigeant que les ministères et organismes du gouvernement fédéral entreprennent une évaluation des facteurs relatifs à la vie privée (EFVP) pour tous les nouveaux programmes ou services qui soulèvent des questions liées au droit à la vie privée. Le Canada est le premier pays dans le monde qui rend obligatoires des EFVP dans tous les ministères et organismes fédéraux.

Pendant plus d'un an avant cette date, le Commissariat avait exhorté le gouvernement à adopter une politique sur l'EFVP, afin de s'assurer que les considérations relatives au droit à la vie privée sont intégrées aux projets dès le départ et non après coup. Nous avons félicité le gouvernement d'avoir mis en application cette politique et d'avoir reconnu que la protection de la vie privée des citoyens est essentielle au succès de tous ses programmes et services, y compris de l'initiative de Gouvernement en direct.

matière de droit à la vie privée de pratiques et de programmes actuels et nouveaux. La Direction des examens et des pratiques en matière de vie privée du Commissariat a participé à de nombreux efforts consultatifs avec les ministères, notamment le Secrétariat du Conseil du Trésor, Elections Canada, Statistique Canada, Développement des ressources humaines Canada, Affaires indiennes et du Nord Canada et Santé Canada.

Ces consultations concernent souvent l'examen de nouvelles propositions relatives à la gestion des renseignements, telles que les initiatives relatives au couplage des données, la création de bases de données et les ententes de partage de renseignements avec d'autres organisations. Il est important de noter que le rôle du commissaire demeure consultatif en ce qui a trait à de telles questions. Le commissaire ne donne, en aucun cas, l'approbation officielle de telles initiatives, ce qui pourrait compromettre son impartialité lors d'enquêtes ou d'examen ultérieurs.

Comme nous l'avons décrit dans nos rapports antérieurs, DRHC a établi un processus d'examen pour traiter des activités d'analyse, de recherche et d'évaluation de politiques qui comportent la connexion de banques de données distinctes. Une partie de ce processus comprend la consultation avec le Commissariat. Au cours de la dernière année, le Commissariat a analysé et commenté près d'une douzaine de présentations de DRHC, dont l'évaluation de l'option Travail partagé de DRHC, l'évaluation des Services d'information sur le marché du travail, l'évaluation des besoins du Programme canadien de prêts aux étudiants et le projet d'ensembles de données relativement au versement de prêt.

Un projet que le Ministère a envoyé au Commissariat, le système d'activités de l'employeur et de l'industrie, a été soumis comme projet concernant les connexions de banques de données. Après examen, le Commissariat a conclu que le projet exigeait plus que la simple connexion des banques de données existantes. Il entraînerait plutôt la création d'une nouvelle banque de données qui serait utilisée de façon continue. On n'a jamais envisagé de traiter de ce genre de projet à travers un tel processus. Par conséquent, nous avons informé DRHC qu'on traiterait de la question de façon plus appropriée

EXAMENS ET PRATIQUES EN MATIÈRE DE VIE PRIVÉE

L'article 37 de la *Loi sur la protection des renseignements personnels* habilite le commissaire à entreprendre des examens de conformité des politiques et des pratiques de gestion des renseignements personnels des institutions fédérales. Cela signifie que le commissaire a la latitude de procéder à des vérifications pour déterminer si elles se conforment aux pratiques équitables en matière de traitement de l'information énoncées aux articles 4 à 8 de la *Loi*. La Direction des examens et des pratiques en matière de vie privée peut évaluer la conformité des organisations aux exigences de la *Loi sur la protection des renseignements personnels*.

Au lendemain du 11 septembre 2001, un certain nombre de ministères et d'organismes fédéraux ont reçu des augmentations considérables de fonds qui leur ont été alloués afin de leur permettre de mettre en œuvre des changements en vue de lutter contre le terrorisme et d'accroître la sécurité nationale. Afin d'évaluer l'incidence de ces mesures antiterroristes sur le droit à la vie privée des personnes, le Commissariat a amorcé cette année des examens des pratiques de traitement des renseignements personnels à la Gendarmerie royale du Canada, au Service canadien du renseignement de sécurité et au Centre de la sécurité des télécommunications. Ces examens seront terminés au cours du prochain exercice.

Un certain nombre de programmes et d'activités établis par des institutions et des organismes du gouvernement fédéral prévoient la communication de renseignements personnels au sujet de citoyens et de résidents canadiens à des départements et organismes du gouvernement des États-Unis. Au cours de cet exercice, le Commissariat a entamé un examen des accords, des ententes et des protocoles conclus entre le Canada et les États-Unis qui prévoient des dispositions pour la communication de renseignements personnels. Dix-huit ministères, départements et organismes ont été sélectionnés pour cet examen, qui sera terminé au cours du prochain exercice. Outre les examens et les vérifications, le Commissariat conseille les organismes fédéraux sur les questions de conformité et les implications en

Lieu d'origine des enquêtes terminées

1^{er} avril 2002 – 31 mars 2003

Province / Territoire		Nombre
Terre-Neuve		14
Ile-du-Prince-Édouard		3
Nouvelle-Écosse		59
Nouveau-Brunswick		52
Québec		2 247
Région de la capitale nationale – Québec		22
Région de la capitale nationale – Ontario		96
Ontario		396
Manitoba		83
Saskatchewan		55
Alberta		167
Colombie-Britannique		273
Nunavut		0
Territoires du Nord-Ouest		0
Yukon		4
Étranger		12
Total		3 483

Demandes de renseignements en vertu de la Loi sur les renseignements personnels

1^{er} avril 2002 au 31 mars 2003 : 5 183

Nous tenterons d'apporter des données détaillées au sujet de ces demandes de renseignements dans nos prochains rapports annuels.

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)

1^{er} avril 2002 – 31 mars 2003

Organisation		Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Société du port de Vancouver	Combattants	2	0	2	0	0	1	5
	Anciens							
	Canada							
	Total	371	77	2 711	76	13	235	3 483

Enquêtes terminées selon les motifs et les résultats

1^{er} avril 2002 – 31 mars 2003

Accès aux renseignements personnels		Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Accès	Correction – annotation	0	1	7	3	0	0	11
	Langue	0	0	0	0	0	2	2
	Frais inexactes	0	0	0	0	0	0	0
	Atteinte à la vie privée	56	4	2 445	17	8	86	2 616
Collecte	Conservation et retrait	7	2	831	2	7	19	868
	Utilisation et communication	4	0	4	0	0	13	21
	Délais	287	1	29	23	0	18	358
	Corrections – délais	2	0	0	0	0	0	2
Délais	Avais de prorogation	12	0	9	0	0	0	21
	Autre	0	0	0	0	0	0	0
	Total	371	77	2 711	76	13	235	3 483

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)

1^{er} avril 2002 – 31 mars 2003

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Ministère de la Justice Canada	4	1	11	1	0	7	24
Archives nationales du Canada	1	0	1	1	0	3	6
Défense nationale	25	7	10	7	1	14	64
Commission nationale des libérations conditionnelles	0	0	1	1	0	3	5
Bureau du directeur général des élections	0	0	0	1	0	0	1
Commissariat aux langues officielles	0	1	0	0	0	1	2
Bureau du Conseil privé	0	1	5	0	0	0	6
Commission de la fonction publique du Canada	1	0	2	0	0	1	4
Travaux publics et Services gouvernementaux Canada	3	0	0	0	0	3	6
Gendarmerie royale du Canada	20	5	41	12	0	28	106
Solliciteur général Canada	0	0	6	0	0	0	6
Statistique Canada	0	0	6	0	0	6	12
Transports Canada	1	2	0	2	0	1	6
Secrétariat du Conseil du Trésor du Canada	0	0	2	0	0	0	2

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)

1^{er} avril 2002 – 31 mars 2003

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Service correctionnel Canada	189	17	42	11	1	65	325
Environnement Canada	0	1	2	3	0	0	6
Financement agricole Canada	1	0	0	0	0	1	2
Ministère des Finances Canada	0	1	0	0	0	0	1
Pêches et Océans Canada	1	3	4	1	0	0	9
Ministère des Affaires étrangères et Commerce international	0	0	5	0	0	0	5
Office de commercialisation du poisson d'eau douce	0	1	0	0	0	0	1
Santé Canada	2	1	6	1	0	1	11
Développement des ressources humaines Canada	19	7	1 568	6	2	6	1 608
Commission de l'immigration et du statut de réfugié	4	4	13	0	0	1	22
Affaires indiennes et du Nord Canada	1	0	2	0	0	3	6
Industrie Canada	0	0	1	0	0	1	2
Bureau de l'inspecteur général du SCRS	0	0	2	0	0	0	2

Enquêtes terminées et résultats selon le ministère ou l'organisme
1^{er} avril 2002 – 31 mars 2003

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Agriculture et Agroalimentaire Canada	2	1	1	2	0	5	11
Agence des douanes et du revenu du Canada	37	14	878	6	8	46	989
Société canadienne d'hygiène des postes	17	4	11	6	0	8	46
Société canadienne d'hygiène des postes	0	0	0	0	0	2	2
Société canadienne d'hygiène des postes	0	0	0	0	0	2	2
Agence canadienne de la personne	1	0	1	0	0	0	2
Agence canadienne de développement international	0	0	0	0	0	0	0
Commission canadienne de sûreté nucléaire	0	0	35	1	0	0	36
Centre canadien du renseignement de sécurité	5	2	18	0	1	0	26
Agence spatiale canadienne	2	0	0	0	0	0	2
Citoyenneté et Immigration Canada	33	4	28	13	0	28	106
Commission des plaintes du public contre la GRC	0	0	5	0	0	0	5

Les dix premiers ministères selon le nombre de plaintes reçues
1^{er} avril 2002 – 31 mars 2003

Organisation	Total	Accès aux renseignements personnels	Délais	Atteinte à la vie privée	Autre
Service correctionnel Canada	456	106	233	117	0
Agence des douanes et du revenu du Canada	205	127	31	47	0
Gendarmerie royale du Canada	200	101	71	28	0
Défense nationale	130	51	58	21	0
Citoyenneté et Immigration Canada	107	52	49	6	0
Développement des ressources humaines Canada	85	38	16	31	0
Société canadienne des postes	71	37	13	21	0
Ministère de la Justice Canada	65	47	13	5	0
Centre canadien du renseignement de sécurité	57	48	8	1	0
Commission canadienne de sûreté nucléaire	36	1	0	35	0
Autres	230	100	50	80	0
Total	1 642	708	542	392	0

À la suite d'une récente enquête menée par le Bureau de l'ombudsman de la Défense nationale, le MDN croyait que les renseignements de RD/DC aideraient le ministère des Anciens Combattants à identifier les anciens combattants qui pourraient avoir droit à des prestations. Les renseignements comprenaient le nom de famille et les initiales de la personne, le nom du produit chimique administré, la date et le lieu de l'administration. On y trouvait aussi quelques numéros matricules mais aucune date de naissance, ce qui rendait impossible pour le MDN d'établir effectivement une correspondance entre toutes les personnes et ses dossiers du personnel.

RD/DC n'avait pas copié ces renseignements dans les états de service ou dossiers médicaux des employés touchés et le MDN espérait que le ministère des Anciens Combattants allait comparer l'information avec ses dossiers afin d'identifier toute correspondance dans son répertoire et communiquer avec les personnes en question. Le but en était que le ministère des Anciens Combattants puisse examiner les cas des anciens combattants qui déclaraient avoir été exposés à des produits nocifs, dont le charbon, mais auxquels on avait refusé toute aide financière parce qu'aucune preuve dans leurs états de service ou dossier médical ne permettait d'appuyer leurs revendications.

L'ancien commissaire a accepté volontiers la décision du MDN. Les avantages pour les personnes étaient évidents ; le ministère des Anciens Combattants pourrait aider à résoudre les questions relatives à l'admissibilité aux prestations en plus d'apporter son aide dans le diagnostic et le traitement des maladies causées par l'exposition aux substances toxiques.

Depuis la Seconde Guerre mondiale jusqu'en 1992, Recherche et développement pour la défense Canada (RDC), une direction générale du MDN anciennement connue sous le nom de Centre de recherches pour la défense, a dressé une liste des membres du MDN qu'elle avait exposés à divers produits chimiques dans le cadre de son programme de recherche sur la guerre chimique. Les membres étaient des volontaires, mais certains d'entre eux n'étaient peut-être pas conscients de leur participation aux expériences.

Toutefois, parmi les 70 avis de communication de renseignements personnels dans l'intérêt public que nous avons reçus durant l'année, un d'eux était clairement justifié : la décision du ministre de la Défense nationale (MDN) de communiquer au ministère des Anciens Combattants des renseignements concernant quelque 2 500 personnes impliquées dans des expériences de guerre chimique.

Il était devenu de plus en plus évident que certaines institutions utilisaient la disposition de façon systématique et courante sans trop penser, à ce qu'il semble, à l'existence d'un intérêt public prédominant à ce moment. Cela était troublant, parce que la situation semblait peu ou pas du tout entrer en ligne de compte dans le processus décisionnel. Souvent, il n'y a eu aucune évaluation pour déterminer ce qui était d'intérêt public et si cet intérêt devrait l'emporter sur les droits à la vie privée de la personne. Étant donné qu'une personne n'a que rarement, sinon jamais, l'occasion de mettre en question la décision, il est essentiel que les décideurs agissent de façon judicieuse et s'assurent de disposer de tous les renseignements pertinents avant de prendre une décision équitable.

L'année dernière, l'ancien commissaire a rappelé à deux ou trois institutions, après avoir examiné leur avis, que la latitude de communiquer des renseignements personnels dans l'intérêt public devrait être réservée aux cas d'aucune autre disposition qui l'autorise dans la Loi.

journalier des recettes et des dépôts et un récépissé des dépôts en espèces. Ces documents identifiaient d'autres personnes et fournissaient leurs numéros de compte, numéros de facture, numéros de carte de crédit et les sommes payées à l'autorité portuaire.

Pour sa défense, l'autorité portuaire croyait n'avoir aucun autre choix que de déposer des documents complets et non révisés avec sa défense pour se conformer au déroulement de l'instance. Dans le cadre de sa défense, elle devait présenter l'information relative à ses opérations financières avec le plaignant et avait l'impression qu'elle ne pouvait retirer aucun renseignement concernant les autres personnes nommées dans ces documents.

Lorsque le Commissariat s'est informé auprès de la cour des petites créances, nous avons appris qu'elle accepterait en fait des documents partiels ou dont des portions ont été retirées. Par conséquent, l'autorité portuaire aurait pu retirer tous les renseignements qui ne concernaient pas le plaignant, dont les renseignements personnels relatifs à d'autres personnes, lorsqu'elle a déposé ses documents au tribunal. Nous avons attiré l'attention de l'autorité portuaire sur cette question et, en conséquence, elle a entrepris de retirer du dossier du tribunal les renseignements concernant les autres personnes. L'autorité portuaire a aussi communiqué avec les personnes concernées pour les informer que leurs renseignements personnels avaient été inclus dans un dossier public.

COMMUNICATIONS DANS L'INTÉRÊT PUBLIC

L'alinéa 8(2)(m) de la *Loi sur la protection des renseignements personnels* autorise le responsable d'une institution gouvernementale à communiquer des renseignements personnels à l'insu et sans le consentement d'une personne concernée dans les cas où un intérêt public clairement prédominant l'emporte sur le droit à la vie privée de la personne ou la personne concernée en tirerait un avantage certain. En vertu du paragraphe 8(5) de la *Loi*, le commissaire à la protection de la vie privée doit être avisé d'avance de toute communication envisagée dans ce cadre.

s'assurer que tous les articles étaient transférés de leur emplacement original au point de chargement, mais que personne n'avait en fait supervisé le transfert de ces articles de cet emplacement à l'endroit où étaient stationnés les fourgons de déménagement à l'extérieur de l'immeuble.

Bien que les ordinateurs n'aient jamais été trouvés, DRHC a été en mesure de déterminer, au moyen de bandes de sauvegarde, qu'ils contenaient les nom et prénom complets, les numéros d'assurance sociale (NAS) et les renseignements médicaux de douzaines de bénéficiaires de prestations d'invalidité du Régime de pensions du Canada (RPC). Par conséquent, DRHC a décidé d'informer ces bénéficiaires du vol.

Durant notre examen de l'incident, nous avons toutefois remarqué que 38 autres personnes dont les noms de famille et NAS figuraient sur des documents n'avaient pas été informées. Étant donné qu'il s'agissait de renseignements personnels suffisants pour peut-être identifier ces personnes, nous avons demandé à DRHC de les informer aussi du vol, ce que le Ministère a fait.

Nous avons aussi recommandé que DRHC établisse des mesures de sécurité supplémentaires pour éviter qu'un tel incident ne se reproduise, plus particulièrement qu'il s'assure de retirer tous les renseignements personnels des lecteurs de disque dur des ordinateurs avant leur déménagement d'un endroit à un autre et de disposer de personnel supplémentaire présent lors des déménagements afin d'offrir une sécurité adéquate en ce qui concerne tout renseignement personnel touché par le déménagement.

Dans un autre incident, une personne a informé le Commissariat que des documents, qu'elle avait reçus de la cour des petites créances à propos des poursuites qu'elle avait intentées contre une autorité portuaire, contenaient des renseignements personnels relatifs à d'autres personnes, en particulier leurs numéros de compte de carte de crédit.

Notre personnel a établi que lorsque l'autorité portuaire avait déposé sa défense à la cour des petites créances, elle avait inclus copie d'un sommaire

Bien que certains secteurs de programme préfèrent ne pas remettre leurs dossiers originaux, tout particulièrement ceux qui concernent des activités administratives en cours, nous leur suggérons d'en garder une photocopie qu'ils peuvent utiliser durant les quelques jours pendant lesquels le bureau de l'AIPRP examine le dossier original. Nous exhortons également les coordonnateurs de l'AIPRP à reprendre leur responsabilité pour la qualité des réponses qu'ils donnent aux personnes en travaillant uniquement avec des dossiers originaux.

Il arrive parfois qu'on attire notre attention sur des incidents de mauvaise gestion de renseignements personnels pour lesquels un examen plus poussé du Commissariat est justifié. L'an dernier, nous avons effectué 32 examens de ce genre.

INCIDENTS VISÉS PAR LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Par exemple, l'été dernier, après le déménagement d'un bureau d'un immeuble à un autre à Ottawa, le personnel de la Direction générale des prestations d'invalidité et des appels de Développement des ressources humaines Canada (DRHC) s'est rendu compte qu'il manquait deux ordinateurs. Bien qu'à la suite d'une enquête menée par sa Division de sécurité DRHC ne fût pas en mesure de déterminer exactement ce qui s'était produit, on croit que les ordinateurs ont été volés alors qu'ils avaient été laissés sans surveillance en attendant d'être chargés dans les fourgons de déménagement. On a suggéré qu'étant donné que les deux ordinateurs étaient neufs, on les avait pris en raison de leur valeur pécuniaire et non de leur contenu. Le vol a aussi été signalé au service de police local, qui n'a pas non plus été en mesure de trouver les ordinateurs manquants ni les auteurs du méfait.

Nos enquêteurs ont établi que les ordinateurs n'avaient pas été emballés dans des boîtes en carton, mais simplement placés sur des chariots sans être protégés d'aucune façon. Ils ont aussi établi qu'un employé de DRHC devait

Traitement de dossiers originaux au lieu de photocopies

Certaines institutions gouvernementales ont refusé à des personnes l'accès à leurs renseignements personnels, contribuant ainsi à l'augmentation du nombre de plaintes adressées au Commissariat, eu égard au fait que les bureaux de l'accès à l'information et de la protection des renseignements personnels (AIPRP) au sein des ministères comptent de plus en plus sur des photocopies que leurs fournisseurs de programme, plutôt que de travailler avec des documents originaux, lorsqu'ils traitent les demandes. Le problème que cela pose est que les analystes de l'AIPRP ne peuvent être certains que ce qu'on leur donne constitue tous les renseignements que souhaite obtenir une personne.

Lorsque le Commissariat reçoit une plainte concernant un « refus d'accès », il demande de voir le dossier original afin de le comparer à l'information traitée au bureau de l'AIPRP. Nous avons souvent constaté que le bureau de l'AIPRP ne disposait pas de tous les renseignements contenus dans le dossier original, parce que quelqu'un avait pensé qu'ils n'étaient pas pertinents ou avait enlevé les notes internes, ou simplement parce qu'on avait oublié le verso de documents recto-verso pendant la photocopie.

Les nuances subtiles qui ne peuvent être appréciées que lorsqu'on regarde un dossier original sont aussi perdues. Les photocopies ne reflètent pas l'utilisation ou la signification de formulaires de différentes couleurs ni n'indiquent la mise en relief de passages importants et peuvent ne pas saisir l'emplacement exact des notes avec commentaires sur papillons adhésifs. Elles ne contiennent pas non plus les trombones qui expliquent pourquoi certains documents sont groupés ensemble ou ne figurent pas dans l'ordre chronologique. Ces éléments sont essentiels pour comprendre le contexte du dossier et déterminer si les renseignements personnels peuvent être fournis à la personne.

L'examen, par nos enquêteurs, des dossiers originaux permet de lever tout doute concernant le fait que l'institution pourrait ne pas avoir trouvé tous les renseignements demandés et nous donne aussi la certitude sans équivoque dont nous avons besoin pour nous assurer que l'accès n'a pas été refusé.

souvent des renseignements personnels concernant d'autres personnes, ne peut être communiquée aux requérants. Le ministère de la Défense nationale est un des organismes qui enregistre les entrevues. Il a récemment fait l'acquisition d'un nouvel équipement dans le but de tenter de simplifier le processus d'examen et de retrait de l'information sur bande.

Les demandes de dossiers d'enquête volumineux expliquent aussi certains retards et difficultés à répondre en temps opportun.

Transmission de renseignements par télécopieur

Bien que nous déconseillions aux institutions d'envoyer des renseignements personnels par télécopieur, nous nous rendons compte qu'elles utilisent régulièrement ce mode de transmission afin d'accélérer la réception de l'information.

Une de nos enquêtes a décelé un problème en ce qui concerne la façon dont une institution gouvernementale gardait un dossier contenant des renseignements personnels envoyés par télécopieur. Les pages couvertures de transmission par télécopieur indiquaient le nombre de pages envoyées, les noms du destinataire et de l'expéditeur, ainsi que la date, mais l'institution ne pouvait déterminer après coup quels documents ou pages en particulier avaient été transmis. Dans d'autres cas, l'institution ne pouvait préciser ce qui avait été reçu par télécopieur d'autres secteurs de l'institution.

Il est impératif que les institutions tiennent un relevé de l'utilisation et de la communication de renseignements personnels qui relèvent d'elles. Sauf dans un nombre limité de cas, les personnes ont le droit de savoir quels documents contenant leurs renseignements personnels sont envoyés, à qui ils sont envoyés et la raison pour laquelle ils sont communiqués.

Une solution à ce problème est de dresser une liste des documents envoyés ou reçus sur la page couverture même de transmission. Cela assurera la transparence, permettra de documenter la circulation de l'information et nous aidera dans nos enquêtes.

Un élément qui continue de nuire à la capacité des institutions de répondre aux demandes dans les délais prescrits est la complexité du traitement des bandes sonores et des bandes vidéo.

Les institutions enregistrent parfois les entrevues menées dans le cadre d'enquêtes administratives ou criminelles. Étant donné que la *Loi sur la protection des renseignements personnels* s'applique aux renseignements personnels « quels que soient leur forme et leur support », les personnes peuvent demander copie de leurs renseignements sur ces bandes. Il s'agit d'un processus qui prend beaucoup de temps ; il faut écouter ou regarder les bandes, puis déterminer et retirer l'information qui, parce qu'elle contient

Agence des douanes et du revenu du Canada :	baisse de 85 à 31 plaintes ;
Développement des ressources humaines Canada :	baisse de 57 à 16 plaintes ;
Service correctionnel du Canada :	hausse de 125 à 233 plaintes ;
Gendarmerie royale du Canada :	hausse de 16 à 71 plaintes ;
Ministère de la Défense nationale :	hausse de 35 à 58 plaintes ;
Citoyenneté et Immigration Canada :	hausse de 40 à 49 plaintes.

Le nombre de plaintes relatives aux délais de réponse de deux institutions ont considérablement diminué par rapport à l'an dernier, tandis que celles concernant quatre autres institutions ont augmenté, à savoir :

opportun.

Plus de plaintes ont été déposées au sujet des pratiques de traitement des renseignements personnels du Service correctionnel du Canada (SCC) que de toute autre institution du gouvernement fédéral. Parmi les 177 plaintes à l'encontre du SCC que le Commissariat a résolues, 159 étaient fondées. Bien que le SCC ait accru son effectif et rationalisé ses procédures, il continue de ne pas répondre aux demandes de renseignements personnels en temps opportun.

ces plaintes, dont 302 étaient fondées.

personnels des citoyens s'élevait à 541 cette année, en comparaison des 428 plaintes signalées au cours de l'exercice antérieur. Nous avons résolu 381 de

Ce renseignement a permis à la personne de se rappeler qu'elle avait fait installer un téléphone au parc. Bien que sa facture téléphonique soit envoyée à sa boîte postale, elle avait dû fournir à la compagnie de téléphone l'adresse du parc pour l'installation et l'entretien de la ligne téléphonique. Il est devenu évident, dès lors, que c'était la compagnie de téléphone et non Statistique Canada qui avait communiqué les nom et adresse de la personne au commissionnaire en publipostage qui, à son tour, avait fourni les renseignements la concernant aux banques.

Au cours de l'enquête, on a demandé au commissionnaire en publipostage de retirer le nom de la personne de la liste de publipostage, ce qu'il a fait immédiatement. Toutefois, la personne a été informée de la possibilité que, bien que son nom ne se trouve plus sur une liste mise à jour, les anciennes listes que détenaient les clients du commissionnaire en publipostage pourraient toujours contenir les renseignements la concernant et par conséquent elle pourrait continuer de recevoir des sollicitations. L'ancien commissaire l'a exhortée à communiquer directement avec ces compagnies afin de faire retirer son nom de ces listes. Il lui a aussi rappelé que son nom pourrait figurer sur d'autres listes à l'avenir si, par exemple, elle faisait une demande de carte de crédit, remplissait un bulletin de participation à un concours ou s'abonnait à des magazines.

Plaintes relatives aux délais de réponse

En vertu de la *Loi sur la protection des renseignements personnels*, les Canadiens et Canadiennes ont le droit d'avoir accès aux renseignements personnels les concernant que détiennent les institutions gouvernementales et, en vertu de la *Loi*, celles-ci doivent répondre dans les 30 jours suivant la réception de la demande. Toutefois, elles peuvent proroger ce délai d'une période maximale de 30 jours, mais seulement dans deux cas précis : le cas où le respect de la période de 30 jours entraverait de façon déraisonnable le fonctionnement de l'institution et le cas où des consultations s'avèrent nécessaires et rendraient pratiquement impossible l'observation de ce délai.

Le nombre de plaintes relatives aux institutions fédérales qui ne répondent pas dans les délais prescrits aux demandes d'accès aux renseignements

renseignements personnels dans la base de données du Registre d'assurance sociale, et qui permettront de mieux surveiller l'accès des employés au Registre. Nous sommes confiants que ces mesures amélioreront la capacité de DRHC de protéger les renseignements personnels dont il est responsable et d'empêcher toute autre atteinte à la vie privée des clients.

DRHC a aussi décidé de soumettre la question à la Gendarmerie royale du Canada en vue d'une enquête criminelle – l'employé a finalement été congédié par DRHC pour l'infraction à la sécurité.

Un recenseur de Statistique Canada trouvé non responsable de la communication de renseignements personnels aux banques

Une personne a allégué que Statistique Canada avait vendu son nom et son adresse à des institutions financières qui lui ont alors envoyé du courrier non sollicité. Cette personne voyageait fréquemment pendant de longues périodes de temps et avait une boîte postale. Elle séjournait dans un parc de véhicules de plaisance au moment du recensement de 2001 et le recenseur lui a expliqué qu'elle devrait utiliser l'adresse du parc pour les besoins du recensement, ce qu'elle a fait. Deux ou trois mois plus tard, elle a commencé à recevoir du courrier non sollicité qui lui était adressé au parc. Étant donné qu'elle avait uniquement utilisé cette adresse pour le recensement, il lui semblait logique que Statistique Canada devait avoir vendu ou sinon fourni l'adresse aux institutions financières.

Nous avons examiné une sollicitation qu'avait reçue cette personne et communiqué avec la banque qui la lui avait envoyée. Au moyen du code inscrit sur la lettre type, la banque a été en mesure de déterminer qu'elle avait obtenu son nom et son adresse au parc de l'une des plus grandes entreprises de gestion de listes au Canada, qui s'occupe de plus de 500 listes de publipostage contenant quelque 25 millions de noms. Ses représentants ont confirmé que les renseignements concernant la plaignante étaient contenus dans une des listes de publipostage créée et mise à jour à partir d'information obtenue de compagnies de téléphone provinciales au Canada.

à une quarantaine d'autres dossiers de clients dans le Registre d'assurance sociale, pour lesquels il n'y avait aucun dossier connexe de DRHC qui aurait exigé que l'employé consulte leurs fichiers de NAS.

L'ancien commissaire était préoccupé du manque de conviction de DRHC relativement au traitement de la plainte de la personne à propos de la communication de son NAS lorsque le Ministère en avait été tout d'abord informé. Il n'a pris aucune mesure autre que de lui émettre un nouveau NAS, en dépit du fait que plusieurs fonctionnaires étaient au

*Mécontent en raison
d'un manque manifeste
de volonté de DRHC de
tenir compte de ses
préoccupations
concernant cette atteinte
à sa vie privée, il s'est
finalement adressé au
Commissariat pour
obtenir de l'aide.*

justifiées comme faisant partie des fonctions d'un employé et pour traiter de cela. DRHC ne surveillent pas régulièrement le Registre d'assurance sociale pour malgré les capacités apparemment adéquates des systèmes, les gestionnaires de Commissariat. L'ancien commissaire était tout aussi préoccupé du fait que, L'ancien commissaire a conclu que DRHC était responsable de la communication inappropriée, par son employé, du NAS de la personne au détective privé et que le Ministère avait, par conséquent, enfreint les dispositions en matière de confidentialité de la Loi sur la protection des renseignements personnels.

En réponse à cette conclusion, DRHC a entrepris de limiter les dégâts autant que possible. Le sous-ministre a envoyé une lettre d'excuses au plaignant et a mis en place des mesures qui amélioreront substantiellement la sécurité des

Communication non autorisée d'un numéro d'assurance sociale (NAS)

Nous avons fait enquête sur une plainte d'une personne selon laquelle Développement des ressources humaines Canada (DRHC) a communiqué de manière inappropriée son NAS à un détective privé.

Le plaignant avait intenté une action en justice contre une compagnie d'assurance qu'il croyait avoir mal traité sa demande d'indemnité. Durant les procédures judiciaires, il a appris que la compagnie d'assurance avait engagé un détective privé pour examiner sa situation financière. Il a obtenu copie du rapport du détective et pris note de références à ses demandes de renseignements adressées à DRHC, de même que l'information qu'il avait reçue par la suite. Mécontent en raison d'un manque de volonté manifeste de DRHC de tenir compte de ses préoccupations concernant cette atteinte à sa vie privée, il s'est finalement adressé au Commissariat pour obtenir de l'aide.

Au cours de l'enquête sur la plainte contre DRHC, nous avons établi qu'un employé de DRHC avait consulté le dossier du plaignant dans le Registre d'assurance sociale au même moment où le détective privé avait soumis ses demandes de renseignements. Bien que le plaignant ait fait part de ses préoccupations à DRHC, le Ministère n'a pas poursuivi davantage la question jusqu'à ce que le plaignant signale son intention d'assigner des employés de DRHC à témoigner au tribunal dans le cadre de sa poursuite intentée contre la compagnie d'assurance. À ce moment, il a demandé copie du dossier d'enquête de DRHC concernant la communication de son NAS et de tout renseignement lié aux mesures prises par DRHC à cet égard. Ce ne fut qu'à ce stade – presque dix mois après que le plaignant avait fait part pour la première fois de ses préoccupations – que DRHC a décidé de faire une enquête interne afin de déterminer si son NAS pourrait avoir été compromis et comment il l'aurait été.

Il est apparu clairement, à partir des éléments de preuve obtenus durant notre enquête, que l'employé de DRHC avait obtenu l'accès au NAS de cette personne sans justification et l'avait communiqué au détective privé. Les preuves ont aussi indiqué la possibilité que l'employé avait d'avoir aussi accès

(RPC) d'une autre personne. Il croit que cette autre personne a probablement reçu ses propres documents d'appel par erreur.

Notre enquête sur cette affaire a confirmé ces craintes. L'autre personne avait en effet reçu de DRHC les renseignements d'appel du plaignant. La confusion résultait d'un manque d'attention au moment où les documents ont été glissés dans les enveloppes avant leur envoi.

L'article 8 de la *Loi sur la protection des renseignements personnels* limite la manière dont les institutions gouvernementales peuvent communiquer des renseignements personnels. En substance, les institutions ne peuvent communiquer de renseignements personnels à des tiers sans le consentement de la personne concernée par les renseignements, à moins qu'un des cas de communication autorisée, énoncés au paragraphe 8(2) de la *Loi*, ne s'applique.

DRHC a expliqué que les renseignements concernant le plaignant qui avaient été communiqués se composaient de documents déposés à la Cour fédérale et faisaient ainsi partie d'un dossier public. Étant donné que le paragraphe 69(2) de la *Loi sur la protection des renseignements personnels* stipule que l'article 8 ne s'applique pas aux renseignements personnels auxquels le public a accès, DRHC a prétendu qu'il n'avait pas enfreint la *Loi* en envoyant par mégarde l'information aux mauvaises personnes.

L'ancien commissaire n'était pas d'accord, parce que les renseignements concernant le plaignant n'avaient pas été communiqués à partir d'un dossier public. Le fait qu'ils se trouvent dans un dossier public n'annule pas la communication par DRHC des renseignements concernant le plaignant à quelqu'un qui n'avait nullement besoin de le savoir. En se fondant sur ce fait, l'ancien commissaire a conclu que la plainte était fondée.

Par suite de la plainte, DRHC a présenté ses excuses aux personnes concernées, leur a envoyé de nouveau les renseignements qui avaient été mal acheminés et a révisé ses procédures d'envoi par la poste afin de minimiser les risques qu'un tel incident se reproduise.

Même un dossier public devrait être protégé

Une personne reçoit une enveloppe par messenger, qui lui est adressée, contenant les documents d'appel du Régime de pensions du Canada

L'ancien commissaire a aussi signalé au SCC qu'il aurait dû aviser nos représentants que l'ami de l'employé avait finalement fait un aveu, après toutes les tentatives infructueuses du SCC et du Commissariat en vue de le retrouver. L'ancien commissaire a jugé qu'il s'agissait là d'un fait extrêmement important, qui a incité le SCC à revenir sur son jugement initial et qui aurait pu, bien évidemment, avoir une incidence directe sur sa décision. Le SCC savait que nous menions une enquête relativement aux allégations du plaignant et, selon l'ancien commissaire, il aurait dû informer immédiatement nos représentants de ce rebondissement. On a assuré l'ancien commissaire que cet oubli était un incident isolé qui ne se reproduira plus.

À la lumière de cet aveu, nous avons mené d'autres interrogations, mais nous n'avons trouvé aucune raison d'accepter la version des faits soutenue par l'ami. Compte tenu des éléments de preuve que nous avons obtenus, l'ancien commissaire a conclu que c'est bien l'employé qui a communiqué les renseignements personnels concernant le plaignant et que son ami n'a probablement fait l'aveu que lorsqu'il est apparu que les répercussions pour l'employé seraient plus graves que prévu. L'ancien commissaire a donc déterminé que la plainte était fondée et demandé au SCC de réexaminer sa décision.

Avant de rendre sa décision finale dans cette affaire, l'ancien commissaire a mis en question les motifs pour lesquels le SCC avait conclu qu'une suspension de trois semaines était une mesure appropriée dans les circonstances. Ce fut à ce moment seulement que nous avons appris que de nouveaux faits avaient incité le SCC à revenir sur sa décision et à annuler la suspension. Conscient de la sanction disciplinaire infligée à l'employé, l'ami de ce dernier avait avoué que c'était bien lui – et non l'employé – qui avait communiqué les renseignements personnels concernant le plaignant. Bien qu'il ne fût pas pleinement convaincu de la crédibilité de l'ami – et qu'il eût des appréhensions à cet égard –, le SCC a décidé d'annuler la suspension.

L'ancien commissaire a reconnu qu'une erreur humaine non sans négligence était à l'origine de ce problème, mais il était consterné par le fait qu'une telle erreur ait pu être commise, surtout par les personnes qui, au sein de l'institution concernée, sont censées être les spécialistes en poste de la protection des renseignements personnels. Si les renseignements personnels de l'employé avaient été traités avec le soin qu'ils méritent, cette grave violation du droit à la vie privée n'aurait jamais eu lieu.

Communication des antécédents criminels d'une personne aux membres de sa famille

Une personne a porté plainte auprès du Commissariat du fait qu'un employé du Service correctionnel du Canada (SCC) a communiqué des renseignements sur ses antécédents criminels à certains membres de sa famille (dont ses jeunes enfants, qui ignoraient tout du passé de leur père), ainsi qu'au grand public. Le plaignant, qui avait été emprisonné quelques années auparavant dans l'établissement fédéral où l'employé travaillait, a accusé ce dernier d'avoir communiqué de l'information confidentielle obtenue dans l'exercice de ses fonctions.

Le SCC a aussi été saisi d'une plainte à ce sujet, et il a mené sa propre enquête. Dès le début, le plaignant a soutenu fermement que l'employé du SCC a communiqué des renseignements personnels le concernant. Ce dernier a maintenu que ce n'est pas lui qui a fait les remarques en question, mais plutôt un ami qui était présent au moment de la communication, ami qu'il a refusé de nommer, tant au cours de notre enquête que lors de celle du SCC. Tous nos efforts en vue de découvrir l'identité de cet ami ont été vains. Néanmoins, compte tenu de tous les renseignements recueillis durant l'enquête, l'ancien commissaire était disposé à conclure que les droits garantis au plaignant aux termes de la *Loi sur la protection des renseignements personnels* avaient été enfreints en raison même des actes de l'employé. De fait, le SCC a déterminé que l'employé avait enfreint le code de discipline de l'institution, ainsi que les dispositions de la *Loi sur la protection des renseignements personnels*, et il l'a suspendu sans solde pendant 15 jours.

Lorsque de tels renseignements ne sont pas traités avec le plus grand soin et avec la plus stricte confidentialité, leur communication peut avoir des conséquences désastreuses.

qu'une vague ressemblance. Pourtant, étant donné qu'il n'a pas pris soin de bien lire les noms des deux personnes, l'analyste du bureau d'accès à l'information et à la protection des renseignements personnels (AIPRP) du ministère a présumé que le requérant et l'employé nommé étaient la même personne. Par conséquent, presque tous les renseignements versés au dossier de dotation ont été communiqués au requérant — seule une petite partie de renseignements relatifs à une tierce personne a été retirée. Le dossier contenait non seulement

enquêtes personnelles sur l'employé nommé au poste.

Après enquête, l'institution a admis promptement son erreur, présentée ses excuses à l'employé et lui a remis une copie des mêmes documents envoyés au requérant, afin qu'il puisse savoir précisément quels renseignements à son sujet avaient été communiqués de manière inappropriée. L'institution a, par ailleurs, demandé au requérant de retourner l'information reçue et de n'en garder aucune copie. Les documents ont bien été renvoyés, mais on ne peut être certain qu'aucune copie n'en a été conservée. D'ailleurs, même si des garanties à cet égard pouvaient être obtenues, le mal est déjà fait, et le requérant a déjà communiqué des renseignements personnels de l'employé à d'autres personnes.

statut des particuliers, notamment en vérifiant si ceux-ci contiennent de réclamer des indemnités aux termes d'un régime d'assurance-maladie provincial pendant leur séjour à l'étranger. En effet, toute personne qui dépose de telles réclamations montre par là qu'elle n'a peut-être pas rompu tous ses liens avec le Canada.

L'ancien commissaire a déterminé que l'ADRC dispose de l'autorité nécessaire, en vertu de la *Loi de l'impôt sur le revenu*, pour recueillir auprès de sources provinciales des renseignements personnels sur tous les membres de la famille dans le but d'établir leur statut de non-résidence. Néanmoins, l'ancien commissaire avait des réserves quant à la *quantité* des renseignements médicaux recueillis, particulièrement en ce qui concerne les renseignements relatifs aux périodes de temps qui se sont écoulées avant et après le séjour de la famille en Afrique. Les responsables de l'ADRC ont convenu qu'il était excessif d'exiger des renseignements médicaux portant sur une période de deux ans et demi après le retour de la famille.

Dans les circonstances, l'ancien commissaire a conclu que l'ADRC avait recueilli plus de renseignements personnels que nécessaire et que, par conséquent, elle avait outrepassé le pouvoir que lui confère l'article 4 de la *Loi sur la protection des renseignements personnels*. Il a déterminé que les plaintes étaient fondées et recommandé que l'ADRC détruise les renseignements obtenus auprès de la province.

Communication par mégarde de renseignements médicaux sensibles par l'AIPRP

Les renseignements personnels sur la santé – ceux qui portent sur notre santé physique et mentale – constituent probablement les données les plus confidentielles qui soient. Lorsque de tels renseignements ne sont pas traités avec le plus grand soin et avec la plus stricte confidentialité, leur communication peut avoir des conséquences désastreuses. L'affaire suivante en est un bon exemple : une personne a présenté une demande en vertu de la *Loi sur l'accès à l'information* (LAI) à une institution gouvernementale visant l'ensemble des documents portant sur la nomination d'un autre employé du gouvernement à un poste donné. Les noms des deux parties ne présentaient

relatifs à l'impôt sur le revenu. Il a expliqué qu'à son avis il est inacceptable qu'on demande à des personnes de produire leurs déclarations de revenus à des fins autres que celles qui sont prévues par la loi. Les Canadiens et Canadiennes ne devraient jamais accepter qu'un de leurs droits fondamentaux soit brimé lorsqu'ils font affaire avec le gouvernement.

Le Commissariat a présenté ces arguments à CIC. En conséquence de quoi, l'ambassade à Manille nous a confirmé qu'elle avait cessé de demander des renseignements relatifs à l'impôt sur le revenu pour la délivrance de visas aux aides familiaux résidents.

Collecte par l'ADRC de renseignements médicaux aux fins de l'impôt sur le revenu

Nous avons reçu une plainte de la part d'une famille qui allègue que l'Agence des douanes et du revenu du Canada (ADRC) a recueilli de

manière inappropriée des renseignements personnels à son sujet auprès d'un fournisseur d'assurance-maladie provincial. Cette famille s'est établie en Afrique pendant trois ans, et avant de quitter le Canada, le mari a consulté l'ADRC, qui l'a informé que, aux fins de l'impôt sur le revenu, il serait considéré comme personne non-résidente durant son séjour à l'étranger. Pourtant, de retour au Canada, il a appris qu'il ne satisfaisait pas aux critères de non-résidence et a donc été imposé en conséquence. Par la suite, après avoir présenté à l'ADRC une demande en vertu de la *Loi sur la protection des renseignements personnels*, il a appris que l'Agence avait demandé à son fournisseur d'assurance-maladie provincial de lui communiquer tous ses dossiers médicaux, ainsi que ceux de sa femme et de ses enfants, notamment des dossiers qui dataient de quelque huit mois avant leur départ pour l'Afrique, et d'autres de près de deux ans et demi après leur retour au Canada.

Nous avons établi qu'une personne ne peut être considérée comme non-résident aux fins de l'impôt que si l'ADRC juge qu'elle a suffisamment rompu ses liens avec le Canada après son déménagement dans un autre pays. L'ADRC s'appuie sur des dispositions de la *Loi de l'impôt sur le revenu* pour recueillir l'information nécessaire en vue de l'évaluation du statut de non-résident. Elle effectue couramment des enquêtes dans le cadre du processus d'évaluation du

relatifs à l'impôt sur le revenu comme condition préalable à la délivrance de visas à leurs aides familiaux éventuels. Les personnes s'inquiétaient du fait d'avoir à envoyer des documents d'impôt contenant leur numéro d'assurance sociale (NAS), ainsi que des renseignements détaillés sur leur situation financière dans un pays étranger, surtout à un moment où l'usurpation d'identité est devenue l'objet d'une si grande préoccupation.

Citoyenneté et Immigration Canada (CIC) a expliqué que le Programme concernant les aides familiaux résidents (PAFR) fait venir au Canada des aides familiaux qualifiés dans les situations où aucun Canadien ou résident permanent ne peut occuper certains postes. Les Canadiens qui souhaitent embaucher un aide familial de l'étranger sont tenus de faire valider leur offre d'emploi par l'entremise de Développement des ressources humaines Canada (DRHC) et de signer un formulaire déclarant qu'ils peuvent subvenir aux besoins de la personne qu'ils emploieront.

Après que l'offre d'emploi a été validée par DRHC, la section des visas de l'ambassade canadienne à Manille a demandé aux employeurs éventuels de lui envoyer leur avis de cotisation des deux dernières années, leurs bordereaux T-4 et une lettre de leur employeur confirmant leur emploi.

CIC a soutenu que l'information était nécessaire pour déterminer l'authenticité d'une offre d'emploi et pour confirmer que les employeurs étaient financièrement en mesure de subvenir aux besoins d'un aide familial. Lorsqu'on a mis en question l'autorité de CIC de recueillir des renseignements concernant l'impôt sur le revenu dans le but de délivrer des visas à des tiers, CIC a fait référence à l'article 203 du *Règlement sur l'immigration et la protection des réfugiés*. Un examen de ce document a indiqué que l'agent des visas doit déterminer si l'offre d'emploi est authentique et si l'emploi du ressortissant étranger aura probablement des retombées économiques neutres ou positives sur le marché du travail au Canada.

Dans le rapport annuel de l'an dernier, l'ancien commissaire a énoncé son point de vue concernant la collecte, sans fondement légal, de renseignements

fédérale a accepté volontairement de prendre des mesures correctives pour remédier à la situation.

Résolue : Il s'agit d'une conclusion officielle qui reflète le rôle d'ombudsman du commissaire. Cette conclusion est réservée aux plaintes pour lesquelles une conclusion *fondée* serait trop sévère dans les cas de mauvaise communication ou de malentendu. Cela signifie que le Commissariat, après avoir mené une enquête complète et minutieuse, a permis de négocier une solution qui satisfait toutes les parties.

Résolue en cours d'enquête : Il ne s'agit pas d'une conclusion officielle, mais d'une façon acceptable de résoudre une plainte. Une fois l'enquête terminée, le plaignant est satisfait des efforts déployés par le Commissariat et consent à laisser tomber l'affaire. Le plaignant retient toutefois le droit de demander qu'une conclusion officielle soit rendue. Le cas échéant, l'enquêteur ouvre le dossier et dépose un rapport officiel. Le commissaire fait alors rapport sur les conclusions dans une lettre au plaignant.

Abandonnée : Il s'agit d'une enquête qui est terminée avant que toutes les allégations ne soient pleinement examinées. Une affaire peut être *abandonnée* pour toutes sortes de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, qui sont essentiels pour en arriver à une conclusion. Le commissaire ne rend pas de conclusions officielles lorsqu'une plainte est abandonnée.

SOMMAIRE DE CAS CHOISIS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

CIC recueillait des renseignements relatifs à l'impôt sur le revenu d'employeurs canadiens

Trois personnes qui souhaitaient employer des aidés familiaux résidents des Philippines se sont plaintes au Commissariat du fait que l'ambassade canadienne à Manille leur a demandé de fournir des renseignements sensibles

tenu de ce fait, l'ancien commissaire était tenu d'informer les plaignants que leurs plaintes étaient non fondées.

Parmi les 1 160 autres plaintes résolues, 486 portaient sur des questions d'accès, 293 concernaient la collecte, l'utilisation, la communication, la conservation et le retrait de renseignements personnels et 381 concernaient les délais prescrits. Les conclusions relativement à ces 3 483 plaintes ont été rendues comme suit :

Non fondées :	2 711
Fondées :	371
Fondées et résolues :	77
Résolues :	13
Résolues en cours d'enquête :	235
Abandonnées :	76

DÉFINITION DE CONCLUSIONS AUX TERMES DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Non fondée : Lorsqu'une plainte est jugée *non fondée*, cela signifie que l'enquête n'a relevé aucun élément de preuve qui porte le commissaire à conclure que l'institution fédérale n'a pas respecté les droits d'un plaignant aux termes de la Loi sur la protection des renseignements personnels.

Fondée : Lorsqu'une plainte est jugée *fondée*, cela signifie que l'institution fédérale n'a pas respecté les droits d'une personne aux termes de la Loi sur la protection des renseignements personnels. Ce serait également la conclusion du commissaire dans une situation où l'institution fédérale refuse d'accorder l'accès à des renseignements personnels malgré notre recommandation qui veut que ceux-ci soient communiqués. En pareil cas, la prochaine étape pourrait consister à demander un recours en révision à la Cour fédérale du Canada.

Fondée et résolue : Le commissaire conclut qu'une plainte est *fondée et résolue* lorsque les allégations sont corroborées par l'enquête et que l'institution

Plus des deux tiers du total des plaintes reçues étaient à l'encontre de cinq institutions du gouvernement fédéral : le Service correctionnel du Canada, l'Agence des douanes et du revenu du Canada, la Gendarmerie royale du Canada, le ministère de la Défense nationale et Immigration Canada.

L'ancien commissaire a rendu des conclusions sur 3 483 plaintes au cours de l'année sur laquelle porte ce rapport. Il est important de noter que ce chiffre comprend 2 323 plaintes liées à la communication, par l'Agence des douanes et du revenu du Canada (ADRC), de renseignements personnels figurant sur les cartes de déclaration douanière E-311 à Développement des ressources humaines Canada (DRHC).

La question en litige portait sur l'autorité nécessaire pouvant justifier l'utilisation de renseignements personnels recueillis par l'ADRC à une fin donnée – pour la déclaration de biens qu'un voyageur apporte au Canada – en vue de l'emploi par DRHC à des fins tout autres, c'est-à-dire dans le cadre d'un programme de couplage de données d'enquête ayant pour but d'identifier les voyageurs de retour au pays qui recevaient frauduleusement des prestations d'assurance-emploi alors qu'ils se trouvaient à l'étranger.

L'affaire a été portée devant un tribunal afin de déterminer si la communication était autorisée en vertu du paragraphe 8(2)(b) de la Loi sur la protection des renseignements personnels et de l'article 108 de la Loi sur les douanes et si l'utilisation de cette information par DRHC comme preuve contre ces personnes enfreignait leurs droits en vertu de la Charte canadienne des droits et libertés.

La Cour suprême du Canada a jugé que la communication était autorisée en fonction de ses interprétations de ces dispositions de la Loi sur la protection des renseignements personnels et de la Loi sur les douanes. Elle a aussi confirmé la décision du tribunal inférieur selon laquelle, en raison de la nature limitée des renseignements communiqués, il n'y avait aucune attente raisonnable quant à la protection des renseignements personnels, décision suivant laquelle, par conséquent, les voyageurs n'avaient pas été privés de leur droit, en vertu de la Charte, d'être protégés contre toute fouille ou saisie déraisonnable. Compte

La Loi sur la protection des renseignements personnels autorise le commissaire à faire prêter serment, à recevoir des éléments de preuve, à pénétrer dans des locaux le cas échéant, à examiner ou à se faire remettre des exemplaires de documents trouvés dans n'importe quel local.

Nous sommes heureux de signaler que nous avons obtenu des collaborations volontaires jusqu'à présent et que toutes les plaintes adressées au commissaire ou à ses prédécesseurs ont été résolues sans que nous n'ayons à invoquer ces pouvoirs d'enquête officiels.

En outre, la Direction des enquêtes et des demandes de renseignements répond chaque année à des milliers de demandes provenant des particuliers et des organisations qui s'adressent au Commissariat afin d'obtenir des conseils et de l'aide pour toutes sortes de questions liées à la protection des renseignements personnels.

Enquêtes terminées sur des plaintes déposées

Du 1^{er} avril 2002 au 31 mars 2003

En 2001-2002 :	1 673
En 2002-2003 :	3 483

Au cours de l'année sur laquelle porte le présent rapport, le Commissariat a reçu 1 642 nouvelles plaintes. Environ 43 % de ces nouvelles plaintes ont été déposées par des personnes alléguant que leur droit d'accès en vertu de la Loi sur la protection des renseignements personnels a été enfreint ; 24% concernaient des alléguations selon lesquelles les dispositions en matière de confidentialité de la Loi en ce qui concerne la collecte, l'utilisation, la communication, la conservation et le retrait des renseignements personnels n'avaient pas été respectées ; les 33 % restants portaient sur la lenteur d'institutions gouvernementales à répondre à des demandes d'accès à des renseignements personnels.

PLAINTES EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

confère la Loi – il peut assigner des témoins à comparaitre et à témoigner, pénétrer dans des locaux afin de se faire remettre des documents et mener des entrevues. L'entrave aux enquêtes constitue une infraction à la Loi. Bien que la Loi ne lui confère pas de pouvoirs de rendre des ordonnances, le commissaire peut, suivant les conclusions d'une enquête, recommander aux institutions fédérales de modifier la manière dont elles traitent les renseignements personnels.

En outre, le commissaire est investi du mandat de mener des vérifications périodiques des institutions fédérales et de recommander des changements aux pratiques qu'il juge non conformes à la Loi.

Aux termes de la Loi, le commissaire est tenu de déposer un rapport annuel au Parlement sur les activités de l'exercice précédent du Commissariat. Le présent rapport vise la période du 1^{er} avril 2002 au 31 mars 2003 au titre de la Loi sur la protection des renseignements personnels.

ENQUÊTES ET DEMANDES DE RENSEIGNEMENTS

La Direction des enquêtes et des demandes de renseignements du Commissariat est chargée de mener des enquêtes sur les plaintes que déposent des personnes aux termes de l'article 29 de la Loi sur la protection des renseignements personnels (et aux termes de l'article 11 de la Loi sur la protection des renseignements personnels et les documents électroniques, dont il sera question plus loin dans le rapport).

Ces enquêtes permettent, essentiellement, de déterminer si les droits à la vie privée des personnes ont été enfreints et si ces dernières ont pu avoir accès à leurs renseignements personnels.

Lorsque les droits à la vie privée et le droit d'accès ont été enfreints, le processus d'enquête cherche à trouver des voies de recours pour les personnes et à empêcher que les violations ne se reproduisent.

Partie I

Rapport concernant la Loi sur la protection des renseignements personnels

INTRODUCTION

La Loi sur la protection des renseignements personnels, qui est entrée en vigueur depuis 1983, assure la protection de la vie privée des personnes en ce qui concerne les renseignements personnels détenus par les institutions du gouvernement fédéral. La Loi régit la manière dont ces institutions recueillent, utilisent, communiquent des renseignements personnels, ainsi que la manière dont elles procèdent à leur retrait, et accorde aux personnes le droit de demander accès à leurs renseignements personnels et celui de demander que des corrections soient apportées. Elle établit en outre les fonctions, les responsabilités et le mandat du commissaire à la protection de la vie privée du Canada.

Le commissaire à la protection de la vie privée reçoit des plaintes de personnes qui estiment que leurs droits aux termes de la Loi ont été enfreints et fait enquête sur ces plaintes. Le commissaire peut également prendre l'initiative d'une plainte et faire enquête lui-même concernant toute situation pour laquelle il a des motifs raisonnables de croire que la Loi a été enfreinte.

En tant qu'ombudsman, la principale priorité du commissaire est de résoudre les plaintes autant que possible, par la médiation et la négociation au besoin. Mais le commissaire possède aussi de vastes pouvoirs d'enquête que lui

Le processus offre

*également une occasion
au public et aux parties*

intéressées de

*commenter la législation
dont il est question.*

chaque année au Parlement du Canada de la « mesure dans laquelle les provinces ont édicté des lois essentiellement similaires à la LRPDE ».

Le commissaire précède à publié deux rapports au Parlement au sujet des lois provinciales essentiellement similaires. En mai 2002, il a publié un rapport dans lequel il a conclu que la Loi sur la

protection des renseignements personnels dans le secteur privé du Québec est essentiellement similaire à la LRPDE en ce qui a trait à la mesure dans laquelle elle protège les renseignements personnels. En juin 2003, le commissaire précède à publié un second rapport dans lequel il a émis des réserves concernant les projets de loi 44 et 38, qui ont été présentés respectivement par les provinces de l'Alberta et de la Colombie-Britannique, mais qui n'ont pas encore été adoptés.

Étant donné qu'aucun de ces projets n'a été adopté, nous continuerons à surveiller leur évolution et maintenir un dialogue avec nos homologues provinciaux.

compétence fédérale, telles les opérations bancaires, la radiotélévision, les télécommunications et les transports.

Le 22 septembre 2001, le ministère de l'Industrie a publié un avis dans la partie I de la *Gazette du Canada* (22 septembre 2001) établissant le processus que le ministère utilisera pour déterminer si les lois provinciales ou territoriales sont réputées être essentiellement similaires.

Le processus sera enclenché par une province, un territoire ou une organisation avisant le ministre de l'Industrie de la loi qui, à son avis, est essentiellement similaire à la *LPRPD*. Le ministre peut aussi agir de son propre chef et recommander au gouverneur en conseil de désigner une loi provinciale ou territoriale comme étant essentiellement similaire.

Le ministre a déclaré qu'il sollicitera le point de vue du commissaire à la protection de la vie privée en vue de déterminer si la législation est essentiellement similaire et il inclura le point de vue de ce dernier dans la soumission au gouverneur en conseil.

Le processus offre également une occasion au public et aux parties intéressées de commenter la législation dont il est question.

Selon l'avis publié dans la *Gazette du Canada*, le ministre s'attend à ce que les lois essentiellement similaires des provinces ou des territoires comportent ce qui suit :

- qu'elles intègrent les dix principes de l'annexe 1 de la *LPRPD* ;
- qu'elles prévoient un mécanisme de surveillance et de recours indépendant et efficace comportant des pouvoirs d'enquête ;
- qu'elles restreignent la collecte, l'utilisation et la communication des renseignements personnels à des fins qui sont appropriées ou légitimes.

En plus de fournir des commentaires au ministre de l'Industrie relativement à la loi spécifique provinciale ou territoriale, le commissaire à la protection de la vie privée est tenu, aux termes du paragraphe 25 (1), de rendre compte

Lois provinciales essentiellement similaires

Aux termes de l'alinéa 26 (2)b) de la Loi sur la protection des renseignements personnels et les documents électroniques, le gouverneur en conseil peut exclure une organisation, activité ou catégorie d'activités de l'application de la LPRPD^É à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels, qui s'effectue à l'intérieur de la province qui a adopté une loi étant réputée être essentiellement similaire à la LPRPD^É.

Le but de cette disposition est de permettre aux provinces et aux territoires de réglementer les pratiques de gestion des renseignements personnels des organisations faisant affaires à l'intérieur de leurs frontières, sous réserve qu'ils disposent d'une loi qui soit essentiellement similaire à la LPRPD^É.

Si le gouverneur en conseil émet un décret déclarant qu'une loi provinciale est essentiellement similaire, la collecte, l'utilisation ou la communication de renseignements personnels par des organisations assujetties à la loi provinciale ne seront pas visées par la LPRPD^É. Néanmoins, les renseignements personnels, qui seront communiqués à l'extérieur de cette province ou du pays seront assujettis à la LPRPD^É, qui contiendra également à s'appliquer, dans les limites d'une province, aux activités des installations, ouvrages entreprises et secteurs d'activité fédéraux qui relèvent de la

L'année nous a donc

apporté quelques bonnes

nouvelles et quelques

déceptions, et de

nombreux défis

toujours à relever.

commissaires à la protection de la vie privée et des données personnelles. Ces différents intervenants nous ont aidé à porter le fardeau des déceptions et on doit leur reconnaître tout le mérite qu'ils ont d'avoir fait leur part pour ce qui est des bonnes nouvelles.

Le Comité permanent des opérations gouvernementales a rempli son devoir en rendant le

Commissariat imputable à l'égard de normes plus strictes en matière de prudence et de probité dans l'utilisation des fonds publics. Alors que nous débutons une autre année décisive en ce qui a trait aux enjeux touchant la vie privée, le Commissariat à la protection de la vie privée s'emploiera à obtenir l'appui renouvelé du Sénat et de la Chambre des communes en vue d'atténuer l'incidence des technologies et des politiques envahissantes, qui portent atteinte aux droits à la vie privée des Canadiens et des Canadiennes.

L'année nous a donc apporté quelques bonnes nouvelles et quelques déceptions et de nombreux défis toujours à relever. Heureusement, nous n'avons pas eu à nous attaquer seuls à nos défis. En effet, la protection du droit à la vie privée nous amène à prendre part à un dialogue permanent, au Canada et à l'étranger, avec des défenseurs du droit de à la vie privée, des défenseurs des libertés civiles, des universitaires et, bien sûr, d'autres

faut en reconnaître la valeur et s'en féliciter.

initiatives gouvernementales viennent renforcer une saine gouvernance, il pourquoi la politique du Conseil du Trésor est si bien accueillie. Lorsque des matière de droit à la vie privée, ce qui est perdu ne peut être retrouvé. C'est concernant une personne ont été soustraits à son contrôle, il est trop tard. En atteinte au droit à la vie privée, lorsque des renseignements personnels celle-ci, plutôt qu'une approche punitive ou réparatrice. De fait, lorsqu'il y a la vie privée, il est plus logique d'adopter une approche préventive comme n'y ait atteinte au droit à la vie privée. À l'égard d'un enjeu comme le droit à communs ou une utilisation accrue de ceux qui existent déjà — avant qu'il ou encore s'il entraîne le recours à de nouveaux identificateurs personnels, couplage de données ou davantage d'échanges de renseignements personnels, droit à la vie privée — à savoir, par exemple, s'il prévoit un nouveau déterminer si un programme ou un projet a une incidence négative sur le L'importance de cette démarche réside dans le fait qu'on cherchera à dès le moment où elles commenceront à planifier un nouveau programme. gouvernements devront tenir compte du droit à la vie privée dès le départ, La mise en œuvre de cette politique implique que les institutions rendre les EFVP obligatoires en ce sens.

renseignements personnels. Le Canada est le premier pays dans le monde à électronique et qui requièrent la collecte, l'utilisation et la communication de qui sont nouveaux, considérablement modifiés ou offerts par voie condition relativement au financement de tous les programmes et services personnels. La nouvelle politique du Conseil du Trésor fait des EFVP une les principes, la loi et les politiques liés à la protection des renseignements communiques, ainsi qu'une évaluation de la conformité du programme avec de ce qu'il adviendra des renseignements personnels recueillis, utilisés et

Nous observons un consensus général autour du fait que le respect du droit à la vie privée n'est pas une tâche aussi onéreuse que certaines personnes l'auraient cru, mais constitue simplement, en fait, une bonne pratique commerciale.

Pour ce qui est des activités quotidiennes, le Commissariat a continué de relever des défis de taille, mais il demeure une organisation solide et performante face à la forte demande du public à l'égard de ses services. Nous avons traité un volume important de plaintes déposées en vertu de la Loi sur la protection des renseignements personnels, avec une hausse de 35 % de nouvelles plaintes cours de la dernière année. En ce qui a trait à la LRPDP, le nombre de nouvelles plaintes a presque triplé au cours de la même période et nous pouvons nous attendre à ce que l'élargissement de l'application de la Loi en 2004 entraîne une augmentation considérable du nombre de plaintes.

Un fait nouveau ayant marqué la dernière année a trait à la présentation de la nouvelle politique du Conseil du Trésor sur les évaluations des facteurs relatifs à la vie privée.

Une évaluation des facteurs relatifs à la vie privée, ou une EFVP, vise simplement à déterminer comment et dans quelle mesure un programme ou une activité comporte des incidences sur le droit à la vie privée des citoyens. Généralement, l'EFVP comporte une description du programme, une analyse

bons résultats en ce qui a trait à la LRPDP. Nous avons été heureux de constater la volonté des organisations du secteur privé assujetties à la Loi de se conformer à ses exigences et de reconnaître l'expertise particulière du Commissariat pour traiter en profondeur les questions liées au droit à la vie privée.

L'année 2003 revêt une importance particulière en ce qui a trait à l'autre loi que nous administrons, la *Loi sur la protection des renseignements personnels* et les *documents électroniques* ou la *LPRPDÉ* comme nous l'appelons, en ce sens qu'il s'agit de la dernière année avant que cette loi ne soit totalement appliquée. En effet, cette loi est entrée en vigueur progressivement. Au départ, soit en 2001, elle s'appliquait à certains échanges de renseignements de nature commerciale, mais elle excluait les renseignements personnels sur la santé. À compter de janvier 2002, son application s'est élargie pour inclure les renseignements personnels sur la santé. L'étape finale débutera en janvier 2004, alors que la *Loi* s'appliquera à toute activité commerciale menée au Canada, sauf dans les provinces où une loi essentiellement similaire aura été adoptée. (Jusqu'à présent, seul le Québec dispose d'une loi sur la protection des renseignements personnels réputée être essentiellement similaire, mais la Colombie-Britannique et l'Alberta ont toutes deux déposé une loi cette année. Ce qui augure bien pour la protection du droit à la vie privée au Canada).

D'une manière générale, l'adoption et la mise en œuvre de la *Loi* se sont déroulées bien plus harmonieusement que certains l'avaient prévu. Le milieu des affaires a bien répondu aux exigences de conformité à la loi et, bien qu'il y ait eu quelques embûches sur la route, la nouvelle façon de faire des affaires n'avait pas été, dans l'ensemble, aussi difficile ou traumatisante qu'on l'avait craint. Nous observons un consensus général autour du fait que le respect du droit à la vie privée n'est pas une tâche aussi onéreuse que certaines personnes l'auraient cru, mais constitue simplement, en fait, une bonne pratique commerciale. Un des signes les plus encourageants réside dans l'intérêt manifeste des gens d'affaires à vouloir se conformer à la *Loi*. En fait, une sorte d'industrie artisanale de la conformité a vu le jour, constituée d'une multitude de sociétés d'experts-conseils offrant leur savoir-faire aux entreprises désireuses de se conformer à la *Loi*. Presque chaque semaine, nous recevons une brochure annonçant la tenue d'un séminaire ou d'un atelier traitant de la *Loi sur la protection des renseignements personnels* et les *documents électroniques*.

De surcroît, le modèle de l'ombudsman, qui a fait ses preuves sous le régime de la *Loi sur la protection des renseignements personnels*, a également donné de

de taille sur les plans financier et pratique quant à sa mise en œuvre et aurait de graves répercussions sur le droit à la vie privée.

Si le Commissariat défend un large éventail d'intérêts et s'efforce d'éclairer le Parlement sur toutes les questions liées au droit à la vie privée, il n'en demeure pas moins que le cœur et l'âme de son travail résident dans le système des droits exécutaires relatifs à la vie privée prévus aux termes de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

À cet égard, l'année 2003 est des plus remarquables. Tout d'abord, elle marque le 20^e anniversaire de la *Loi sur la protection des renseignements personnels*. Ce qui nous porte à réfléchir non seulement sur la dernière année, mais aussi sur les vingt dernières années et tout particulièrement sur le modèle de protection du droit à la vie privée sous la régime de la *Loi sur la protection des renseignements personnels* adoptée par le Parlement. Ce modèle repose sur la nomination d'un haut fonctionnaire du Parlement, le commissaire à la protection de la vie privée, qui conseille le Parlement sur des questions en matière de vie privée, analyse les répercussions des initiatives en matière de législation et de réglementation de manière à ce que les membres du Parlement ainsi que les Canadiens et les Canadiennes soient en mesure de prendre des décisions éclairées, et agit comme ombudsman en vue de protéger les droits à la vie privée, et ce, en recourant à la négociation, à la persuasion et au dialogue, et parfois, en dernier ressort, à la publicité. Le système mis en place aux termes de la *Loi sur la protection des renseignements personnels* s'est rapidement révélé utile et nul n'a été surpris qu'il ait été approuvé et mis en application dans le secteur privé lorsque le Parlement a adopté la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Nous sommes confiants que, durant la dernière année, le Parlement a su tirer parti de ce système et que, à vrai dire, son utilité a été réaffirmée. Le Parlement a repensé et révisé des initiatives législatives, comme le projet de base de données de l'ADRC, pour réduire au minimum ses répercussions sur le droit à la vie privée. À notre avis, l'avenir du droit à la vie privée au Canada s'annonce bien malgré toutes les pressions subies.

Au cours de la dernière année, nous avons été frappés par le fait que bon nombre de nos préoccupations en matière de vie privée étaient liées à l'anonymat et à son pôle contraire, l'identité. La capacité de mener la plupart de nos activités quotidiennes dans l'anonymat est un des moyens dont nous disposons pour exercer un contrôle sur les renseignements qui nous concernent. Une personne peut bien avoir une vie privée même si elle passe le plus clair de son temps en public, pourvu que ses activités ne puissent pas être reliées entre elles et qu'aucun lien ne puisse pas être établi entre cette personne et ses activités. La capacité de relier des activités entre elles et de les relier à une personne identifiable constitue l'essentiel de l'établissement de profils et de la surveillance.

Cette perspective regroupe les préoccupations que nous avons à l'égard de questions différentes en apparence, telles que l'authentification des clients effectuant des transactions électroniques, les systèmes biométriques de reconnaissance des visages dans les aéroports, les bases de données sur les voyageurs et la carte d'identité nationale.

C'est là l'idée que nous avons tenté de faire valoir devant le Comité permanent de la citoyenneté et de l'immigration de la Chambre des communes lors des audiences portant sur la question de savoir si le Canada a besoin d'instituer une carte d'identité nationale. Nous avons fondé notre argument sur le fait qu'une telle carte (quels que soient les détails de la proposition, et aucune proposition réelle n'a encore été présentée) aurait peu d'incidence sur le règlement des vrais problèmes, qu'elle présenterait un défi

pairs et aux personnes qui désirent effectuer des recherches généalogiques sur leur propre famille. Le gouvernement a rejeté l'idée.

Ce qui nous préoccupe, c'est la promesse répétée de confidentialité. On a demandé aux Canadiens et aux Canadiennes de révéler des renseignements personnels aux recenseurs en leur laissant croire que tout demeurerait confidentiel. Le non respect de cette promesse pourrait diminuer la confiance que les Canadiens et les Canadiennes ont envers le gouvernement. Nous continuons d'espérer que la Chambre des communes tiendra compte de ce fait lorsqu'elle reprendra ce projet de loi, que le Sénat a adopté en mai.

En ce qui a trait à la surveillance vidéo des voies publiques, un autre enjeu important en matière de vie privée, nous avons conclu qu'il était essentiel d'adopter une nouvelle approche. L'ancien commissaire avait intenté un procès devant la Cour suprême de la Colombie-Britannique, alléguant que la surveillance vidéo, par la GRC, d'une rue publique de Kelowna contrevenait aux dispositions de la *Charte canadienne des droits et libertés*. Toutefois, le juge ne s'est pas du tout intéressé au fond de l'affaire. Statuant que le commissaire à la protection de la vie privée n'était simplement pas habilité à entamer une telle poursuite, il a rejeté l'affaire.

Nous nous trouvions donc dans une situation délicate. D'une part, la surveillance vidéo de lieux publics a de graves répercussions sur le droit à la vie privée, de sorte que l'idée de laisser simplement tomber l'affaire en raison d'un problème procédural ne nous semblait guère satisfaisante. D'autre part, peu importe ce que nous voulions, l'enjeu était devenu celui que la Cour avait adopté. Si nous avions appelé de la décision, l'appel n'aurait porté que sur ce point. Il nous aurait fallu des années pour traverser deux autres niveaux d'appel et ces procédures auraient nécessité beaucoup d'énergie de la part du Commissariat, ainsi qu'une quantité considérable de fonds publics, et ce sans que nous puissions obtenir des tribunaux une réponse sur l'enjeu essentiel de la surveillance vidéo. Certes, il est impératif de s'attaquer à la question, mais nous devons nous y prendre autrement. Par conséquent, nous avons abandonné l'action en justice, mais nous poursuivrons cette affaire avec détermination.

Mais il faut plus qu'une réussite pour qu'une année soit exceptionnelle. Nous avons toujours des préoccupations concernant d'autres initiatives liées à la sécurité. Pensons notamment aux dispositions du projet de loi sur la sécurité publique permettant aux policiers de contrôler tous les passagers des transporteurs aériens au regard des mandats d'arrestation non exécutés ; aux propositions relatives à « l'accès légal » visant à accroître les pouvoirs de l'État en matière de surveillance des communications électroniques ; à la proposition concernant la carte d'identité nationale et au recours croissant par les forces policières à la surveillance vidéo des voies publiques.

Un conflit de longue date, entourant la confidentialité des données de recensement, semble en voie d'être résolu d'une manière qui va tout à fait à l'encontre des recommandations du Commissariat.

Depuis au moins 1905, on répète aux Canadiens et aux Canadiennes que les renseignements fournis dans le cadre des recensements demeurent confidentiels et servent uniquement à des fins statistiques. En fait, la *Loi sur la protection des renseignements personnels* permet aux Archives nationales de communiquer des renseignements personnels recueillis dans le cadre d'un recensement, 92 ans après que ce dernier a été réalisé. Cette disposition est demeurée en grande partie purement théorique jusqu'à tout récemment, dans la mesure où les seules données de recensement dont disposaient les Archives provenaient des quelques recensements effectués jusqu'en 1901. Les fonctionnaires du recensement ont affirmé que, depuis le recensement de 1906, les lois et les règlements les obligeaient à conserver les données confidentielles plutôt que de les transférer aux Archives.

Les historiens et d'autres chercheurs ont longtemps sollicité l'accès à ces documents. Or, cette année, le gouvernement, suivant les recommandations formulées par un groupe d'experts mais passant outre nos objections, a rendu publiques les données du recensement de 1906 et adopté une loi permettant la communication des données des autres années.

Le Commissariat avait favorisé un compromis qui aurait limité l'accès aux données aux chercheurs qui mènent une étude historique examinée par des

*À l'égard de questions
d'ordre plus général liées
à la promotion et à la
protection du droit à la
vie privée, nous avons
réalisé quelques
progrès significatifs.*

significatifs. Nous avons aussi
connu certains reculs et, dans
quelques domaines, nous avons
été forcés de repenser notre
approche.

Cette base de données, telle que
proposée au départ, devait contenir des
renseignements très détaillés sur les voyages à l'étranger effectués par les
Canadiens et les Canadiennes — où et avec qui ils voyagent, comment ils
ont payé leurs billets, leurs adresses et numéros de téléphone et même leurs
besoins particuliers en matière d'alimentation et de santé. On aurait conservé
pendant sept ans cette information, qui aurait servi à un vaste éventail
d'objectifs administratifs et d'objectifs liés à l'application de la loi.

Les répercussions de ce projet auraient été considérables et sans précédent.
Des voyageurs respectueux de la loi auraient vu leurs activités habituelles, qui
auparavant seraient passées inaperçues à moins qu'il n'y ait eu des motifs
valables de s'en méfier, consignées et conservées dans un fichier à leur nom.
Il en résulterait une autre perte de l'anonymat et du droit à la vie privée, un
autre moyen pour l'État d'identifier, d'étiqueter et de surveiller des personnes
innocentes, bref une autre atteinte au droit à la vie privée.

Après avoir analysé ce projet, notre personnel a conclu que les avantages
supposés qu'il allait offrir sur le plan de la sécurité ne justifiaient pas la
violation du droit à la vie privée qui allait en découler. Notre opposition, qui
a reçu l'appui du public, a finalement incité la ministre du Revenu national à
revoir le projet et, ce faisant, à en réduire considérablement l'incidence sur le
droit à la vie privée.

posent également un défi des plus indéniables pour les défenseurs du droit à la vie privée et les commissaires à la protection de la vie privée qui, ce faisant, doivent tenir une position délicate entre la protection du droit à la vie privée et le risque de faciliter la vie des criminels et des terroristes.

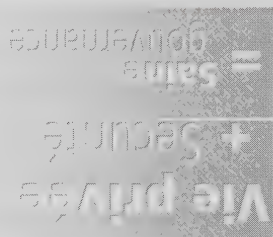
Mais, en fait, les autres forces qui menacent la vie privée ne posent pas moins de défi et le fait d'avoir à y faire face et d'œuvrer en faveur du droit à la vie privée nous met souvent dans des situations tout aussi délicates. Le couplage des données permet d'appréhender les personnes qui tentent de frauder le système. Les cartes d'identité peuvent rendre la tâche plus difficile à une personne qui cherche à utiliser frauduleusement votre carte de crédit. Les dossiers de santé électroniques peuvent faciliter le diagnostic et le traitement des maladies et prévenir des erreurs médicales pouvant entraîner des coûts importants ou causer la mort. Le fait de donner aux chercheurs accès aux renseignements personnels sur la santé peut donner lieu à des recherches en vue de prolonger la vie et réduire la souffrance.

Personne ne contesterait les objectifs de ces mesures. Mais le droit à la vie privée n'est pas simplement un luxe ou une extravagance égoïste que l'on peut jeter dès que quelqu'un prétend qu'elle est une entrave à quelque autre objectif social important, qu'il s'agisse de la sécurité ou de la santé publique ou même de la vie personnelle ou de la mort. Le droit à la vie privée est la pierre angulaire de la liberté individuelle. Elle forme un équilibre dynamique avec les autres besoins sociaux que nous avons. Pour préserver le droit à la vie privée, il importe d'analyser minutieusement toute mesure censée nous procurer quelque autre avantage social, de manière à s'assurer que l'équilibre est maintenu.

Au cours de la dernière année, nos efforts ont donné des résultats divers. Nous avons continué de gérer un volume important de plaintes et de veiller à ce que les Canadiens et les Canadiennes jouissent d'une pleine protection de leurs droits en vertu de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et les documents électroniques*. À l'égard de questions d'ordre plus général liées à la promotion et à la protection du droit à la vie privée, nous avons réalisé quelques progrès

Aperçu

Il est habituel de faire la présentation d'un rapport annuel en formulant quelques observations afin de susciter la réflexion. Dans le cas du présent rapport, il ne s'agit pas d'une présentation futile. La période couverte s'est avérée particulièrement importante pour le droit à la vie privée.



D'une part, le droit à la vie privée dans notre société a été quelque peu menacé. Ce qui n'est certes pas nouveau ; le droit à la vie privée n'a jamais été quelque chose que nous pouvons prendre pour acquis, et cela est d'autant plus vrai depuis l'avènement de l'informatisation, qui nous force à tout mettre en œuvre pour le préserver. Mais si la menace qui plane sur le droit à la vie privée n'est pas nouvelle, elle s'est bel et bien accentuée. Les forces qui rongent le droit à la vie privée depuis dix ans — les avancées technologiques liées à la collecte, au traitement, au couplage et à l'analyse des renseignements personnels, la pression grandissante exercée pour que l'on identifie et authentifie les parties à des transactions électroniques et la campagne de prévention du crime et du terrorisme — ont été particulièrement puissantes au cours de la dernière année.

Les mesures de sécurité publique pour lutter contre le crime et le terrorisme ont sans aucun doute constitué le défi le plus grave et le plus évident. Elles

Pour compiler les choses, le Commissariat a traversé une période durant laquelle il a fait l'objet d'un examen public minutieux et connu des perturbations organisationnelles. Le Comité permanent des opérations gouvernementales et des prévisions budgétaires de la Chambre des communes a mené une enquête relativement à diverses questions opérationnelles et administratives qui se sont posées au Commissariat et il a relevé un certain nombre de problèmes sérieux. Bien que ce processus de supervision parlementaire soit important et nécessaire, on ne saurait nier le fait qu'il a rendu difficile la tâche du personnel du Commissariat de mener à bien son travail, surtout si l'on considère l'attention médiatique qui l'a accompagné.

J'ai accepté le poste de commissaire à la protection de la vie privée à titre intérimaire, afin de conduire le Commissariat dans son processus de reconstruction et de restauration des liens qu'il entretenait avec le Parlement et la population canadienne. Nous avons maintenant pour tâche de regagner la confiance du Parlement et des intervenants en matière de vie privée, de prouver aux Canadiens et aux Canadiennes que nous sommes en mesure de leur fournir des services de haute qualité en ce qui a trait à la protection de leurs droits à la vie privée, de veiller à ce que les organisations comprennent leurs obligations et les citoyens leurs droits, lorsque la *Loi sur la protection des renseignements personnels et les documents électroniques* entrera pleinement en vigueur le 1^{er} janvier 2004.

J'ai été impressionné par l'engagement des employés du Commissariat et je suis heureux de collaborer avec eux en cette période stimulante de l'histoire de l'organisme. Je demeure confiant qu'un regain d'enthousiasme pour la défense du droit à la vie privée et un centre d'excellence pour sa protection et sa promotion naîtront de cette période de renouveau.

Préface



D'aucuns trouveront peut-être singulier que ce soit moi qui présente le rapport annuel de l'exercice 2002-2003. En effet, j'ai été nommé commissaire à la protection de la vie privée par intérim en juillet de cette année bien après la fin de la période visée par ce rapport. Je ne peux, par conséquent, m'attribuer le mérite des travaux rapportés ici. Cependant, à y regarder de près, cette situation ne pose pas vraiment problème. Le Commissariat à la protection de la vie privée ne se limite pas au commissaire, et d'ailleurs, même si j'avais occupé mes fonctions actuelles tout au long de l'exercice 2002-2003, il serait illusoire de dire que ce rapport est « mon » rapport annuel. Il reflète plutôt le travail de personnes très talentueuses et dévouées.

Le Commissariat traverse une période particulièrement mouvementée de son histoire. *A priori*, la tâche de la protection de vie privée est plus ardue que jamais, en raison de la nouvelle loi pour le secteur privé, d'un vaste éventail de mesures proposées en matière de sécurité et de lutte contre le terrorisme, et de la propagation de technologies sans cesse améliorées qui portent atteinte à la vie privée.

Table des matières

Préface.....	1
Aperçu.....	3
Lois provinciales essentiellement similaires	15
Partie I - Rapport concernant la Loi sur la protection des renseignements personnels	19
Introduction.....	19
Enquêtes et demandes de renseignements	20
Plaintes en vertu de la Loi sur la protection des renseignements personnels.....	21
Définition de conclusions aux termes de la Loi sur la protection des renseignements personnels.....	23
Sommaires de cas choisis en vertu de la Loi sur la protection des renseignements personnels.....	24
Incidents visés par la Loi sur la protection des renseignements personnels.....	39
Communications dans l'intérêt public	41
Examens et pratiques en matière de vie privée.....	50
Évaluation des facteurs relatifs à la vie privée.....	52
Devant les tribunaux	57
Partie II - Rapport concernant la Loi sur la protection des renseignements personnels et les documents électroniques	63
Introduction.....	63
Enquêtes et demandes de renseignements.....	64
Définition de conclusions en vertu de la LPRPD.....	65
Sommaires de cas choisis en vertu de la LPRPD.....	66
Incidents visés par la LPRPD	101
Examens et pratiques en matière de vie privée	104
Devant les tribunaux	105
Partie III - Services de gestion	111



Septembre 2003

L'honorable Peter Milliken, député
Président
Chambre des communes
Ottawa

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat
à la protection de la vie privée du Canada pour les périodes du 1^{er} avril 2002 au
31 mars 2003 conformément à la Loi sur la protection des renseignements personnels
et du 1^{er} janvier au 31 décembre 2002 conformément à la Loi sur la protection des
renseignements personnels et les documents électroniques.

Vous le saluez agréé, Monsieur, l'expression de mes sentiments distingués.

Commissaire à la protection
de la vie privée du Canada
par intérim,

Robert Marleau

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tél.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télé.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



Septembre 2003

L'honorable Daniel Hays, sénateur
Président
Sénat du Canada

Ottawa

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour les périodes du 1^{er} avril 2002 au 31 mars 2003 conformément à la Loi sur la protection des renseignements personnels et du 1^{er} janvier au 31 décembre 2002 conformément à la Loi sur la protection des renseignements personnels et les documents électroniques.

Veuillez agréer, Monsieur, l'expression de mes sentiments distingués.

Commissaire à la protection
de la vie privée du Canada
par intérim,

Robert Marleau

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-8210, 1-800-282-1376
Téléc. (613) 947-6850
ATS (613) 992-9190

© Ministre des Travaux publics et Services gouvernementaux Canada 2003
N° de cat. IP30-1/2003
ISBN 0-662-67544-4

Cette publication est également disponible sur
notre site Web à www.privcom.gc.ca

AU PARLEMENT 2002-2003

RAPPORT ANNUEL

Vie privée

Commissaire à la protection
de la vie privée du Canada



Privacy Commissioner
of Canada

AU PARLEMENT 2002-2003

RAPPORT ANNUEL

Vie privée

Commissaire à la protection
de la vie privée du Canada



Privacy Commissioner
of Canada

Privacy Commissioner
of Canada



Commissaire à la protection
de la vie privée du Canada

CA1
PC
- A57

Privacy

**Annual Report to Parliament
2003-2004**



Privacy Commissioner
of Canada



Commissaire à la protection
de la vie privée du Canada

Annual Report to Parliament 2003-2004



Canada



Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2004
Cat. No. IP50-2004
ISBN 0-662-68421-4

This publication is also available on our Web site at www.privcom.gc.ca

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



November 2004

The Speaker

The Honourable Daniel Hays, Senator
The Senate of Canada
Ottawa

Dear. Mr. Speaker:

I have the honour to submit to Parliament the Annual Report for the Office of the Privacy Commissioner of Canada, for the period from April 1, 2003 to March 31, 2004 for the *Privacy Act* and from January 2 to December 31, 2003, for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".

Jennifer Stoddart
Privacy Commissioner of Canada

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



November 2004

The Honourable Peter Milliken, M.P.
The Speaker
The House of Commons
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report for the Office of the Privacy Commissioner of Canada, for the period April 1, 2003 to March 31, 2004 for the *Privacy Act* and from January 1 to December 31, 2003 for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

Foreword	1
Overview	5
Policy Perspective	13
Substantially Similar Provincial Legislation	21
Part One – Report on the <i>Privacy Act</i>	25
Introduction	25
Investigations and Inquiries	26
Complaints under the <i>Privacy Act</i>	26
Definitions of findings under the <i>Privacy Act</i>	27
Select cases under the <i>Privacy Act</i>	28
Incidents under the <i>Privacy Act</i>	35
Public interest disclosures under the <i>Privacy Act</i>	36
Privacy Practices and Reviews	46
Privacy Impact Assessments	52
In the Courts	54
Part Two – Report on the <i>Personal Information Protection and Electronic Documents Act</i>	57
Introduction	57
Investigations and Inquiries	57
Definitions of findings under <i>PIPEDA</i>	58
Select cases under <i>PIPEDA</i>	59
Incidents under <i>PIPEDA</i>	80
Privacy Practices and Reviews	83
In the Courts	84
Part Three – Corporate Services	95

FOREWORD

This has been an exceptional year for the Office of the Privacy Commissioner of Canada. When I was appointed on December 1, 2003, I took over stewardship of an office that had undergone a great upheaval. In the course of six months, a Commissioner and several senior officials resigned amid scandal and intense publicity, an interim Commissioner was appointed, numerous internal and external reviews, audits and investigations were undertaken – and some are still ongoing – two Assistant Privacy Commissioners were appointed and a significant corporate restructuring was undertaken. I took over the helm of a ship that, while set on a positive course by Interim Privacy Commissioner Robert Marleau, was still navigating through a sea of administrative, financial and organizational crises.



Great progress has been made in the institutional renewal and strengthened management and financial framework of the OPC. This progress has been essential to rebuilding this Office and our efforts to emerge as a more effective organization, which upholds the principles of the Public Service while, at the same time, delivering on its mandate to protect and defend the fundamental privacy rights of Canadians.

I would like to salute the tremendous work of Interim Commissioner Robert Marleau in helping to move this Office through a difficult and complex period. M. Marleau's support and encouragement of staff, his work with audit and investigation teams and his emphasis on responsibility and teamwork have provided a strong foundation for a return to normalcy. He has our appreciation and gratitude.

In building on that foundation, corrective measures have been taken and continue to be taken to restore the overall wellness of the working environment, to further strengthen management practices and financial controls, to bring greater transparency and fairness to the human resources function, to encourage innovation, and to engage employees and union representatives in re-building and sustaining a process of organizational learning.

Other measures successfully undertaken include a cost recovery plan and a comprehensive planning process to realign our strategies and goals. An initial Report to Parliament on Action Arising from the Auditor General's Report on the Office of the Privacy Commissioner of Canada, jointly tabled by our Office and the President of Treasury

Board of Canada on October 31, 2003, detailed actions taken or to be taken on recovery actions by our Office. The report was followed by a final report tabled in April 2004.

We have also established an External Advisory Committee comprised of distinguished national privacy experts to provide input and guidance to the Office on strategic directions and priorities and established a Union Management Consultation Committee and a Health and Safety Committee to restore the overall wellness in the workplace. In addition, we are working actively with the Treasury Board Secretariat to improve our Human Resources functions. A significant focus of our renewal has been to re-build and regain the confidence of the Parliament of Canada. To this end, we have created a new role for a Parliamentary Liaison Officer, to help us fulfill our ongoing responsibilities as Parliament's window on privacy issues.

In the midst of this challenging and chaotic year, our Office was preparing for full implementation of the *Personal Information Protection and Electronic Documents Act* — also known as *PIPEDA*. On January 1, 2004, *PIPEDA*, which has come into force in stages, extended to the collection, use or disclosure of personal information in the course of any commercial activity within a province — except where privacy legislation deemed “substantially similar” by the federal government is in force.

PIPEDA is a flexible, pragmatic law that addresses the multi-jurisdictional issues raised in our constitutional context. The *Act* may be replaced by legislation that has been found to be “substantially similar” to the federal law. At the time of publication of this report, only Quebec's legislation has been found to be substantially similar, although we expect positive findings for the privacy legislation passed in Alberta and British Columbia. Our Office is working and will continue to work cooperatively with our provincial counterparts in a harmonized approach to dealing with privacy complaints in the private sector.

PIPEDA thus affects organizations from large corporations to small convenience stores, multi-national financial and insurance industries to corner florists and the neighbourhood dry cleaners. There has been an initial period of confusion and anxiety over these new rules about personal information in the private sector.

However, over the year and particularly in the months leading up to the January 1, 2004 target date, our focus was to help organizations implement and comply with *PIPEDA* and to engage in outreach, cooperation, public education, and the creation of innovative new partnerships with the private sector. We have consulted extensively with private sector business associations, in particular with the banking and financial sector and with the direct marketing industry. Assistant Privacy Commissioner Heather Black,

former General Counsel with our Office and with Industry Canada, where she worked on development of the *Personal Information Protection and Electronic Documents Act*, has criss-crossed the country this year on a busy schedule of speaking engagements to a wide variety of groups to raise awareness about *PIPEDA*.

We also responded to thousands of inquiries and requests for information on *PIPEDA* from businesses and organizations all across Canada; we engaged in consultations with business groups and associations; we sent out thousands of copies of reports, business guides, fact sheets and other public education materials; we have reorganized and overhauled our Web site to be compliant with the Government Common Look and Feel standards, and have made several new resources, guides and compliance tools available electronically to Canadian businesses and individuals.

It has been an exceptional year for *Privacy Act* complaints as well. Our Office received a record number of new complaints — a 250 per cent increase over the previous year. You will find more details explaining these statistics further on in this Report. As well, our investigators closed a record number of complaint investigations — an achievement to be highly commended in light of the extra challenges faced by our staff this year.

While it has been a difficult and challenging time for our Office, our work to monitor technological trends and initiatives to help protect Canadians' privacy and the integrity of personal information continued, with new threats to privacy emerging nationally and internationally. At the start of the year, the idea of a National Identity Card was proposed, opposed by many Canadians, and has been put on hold — for the time being at least. The vast majority of Canadians who made presentations to the Committee — including representatives from this Office — were staunchly opposed to the introduction of a national identity card. We remain opposed.

Personal information about Canadians continued to be gathered, stored, sorted and shared in alarming amounts on the basis of the idea — however unproven — that more information about individuals equals greater security against terrorists and other threats. We are concerned about the increasing integration of our border security with that of the United States, and the impetus this gives to the collection of large databases of personal information about travellers, potential travellers, and people in the transportation industry who must cross borders regularly to do their jobs. Our Office is looking very closely at the personal information handling practices of the newly created Canadian Border Services Agency.

The issue of trans-border data flow also commanded our specific attention this year. In an increasingly digital world, Canadians' personal information can be sent anywhere in the world

at the click of a mouse. We are concerned about the impact this may have on Canadians' rights to privacy. Our Office is working on a project that will help outline the pathways for personal information flow across borders, and what rights and protections may apply to that information. We recognize the need for increased security in today's environment, and would never stand in the way of legitimate measures to fight terrorism. But the need for national and international security must be balanced against the fundamental human right to privacy and the individual's right to control the collection, use and disclosure of personal information.

New technologies are emerging that threaten our privacy in ways previously unimagined. We will continue to monitor the use and impact of technologies such as video surveillance, spyware, radio frequency identification devices (RFIDs), global positioning systems, wireless communication devices, and biometric identifiers such as face recognition, DNA and fingerprints. Our Office is working with our federal partners on finding appropriate legal, regulatory, and technical measures to address these issues.

For example, we have seen spam – those ubiquitous unsolicited e-mail messages – rapidly become a real risk to Canadians' privacy and the integrity of their personal information. Spam messages often carry malicious computer code into your computer system, creating programs that can read your e-mail, track your Internet use, and even steal your passwords and credit card numbers. Our Office is working closely with Industry Canada and its anti-spam task force to develop ways to tackle this insidious problem, and to help consumers take pro-active measures to protect themselves. Similarly, we will pursue opportunities to protect the privacy rights of consumers in dealing with the potential negative impact of new technologies that pose privacy concerns.

In the coming year, our Office will continue to focus on outreach and communications to help Canadian individuals and businesses to understand their rights and obligations under the *Privacy Act* and *PIPEDA*. We continue to seek input from Canadians in a variety of ways to help us better serve their needs, and to help strengthen the Office of the Privacy Commissioner as a seminal force in protecting and promoting privacy rights.

Above all, I would like to take this opportunity in my first report as Privacy Commissioner to praise the staff of this Office, which has laboured under unprecedented challenges, personally and administratively, to get the work done. I commend them for their professionalism, their dedication to upholding privacy rights for Canadians, for upholding the principles of the Public Service and for their grace under pressure. It has been a difficult year, but, as the saying goes, crisis creates opportunity. I am proud to say this Office has seized the opportunity to rebuild on a stronger foundation, and is confidently moving forward with renewed energy to meet the many privacy challenges ahead.

By most measures, the past year was a challenging year for privacy. As threats to privacy proliferated, the fight to protect the privacy rights of Canadians and to protect personal information was at times an uphill battle. The outlook however is not entirely bleak.

Surreptitious surveillance technologies

Every day, we read media stories about new technologies, or new uses of existing technology, that threaten our privacy. Global positioning systems that track the location and movements of vehicles by satellite are being installed in rental cars and in employees' vehicles. Cell phone cameras that can surreptitiously capture and transmit images of people are being used to violate the privacy of individuals. An increasing number of municipalities are considering installing video surveillance cameras in their downtown areas.

During the past year, we have become familiar with the term “radio frequency identification chips” or “RFIDs”. These miniature computer circuits outfitted with tiny antennae that vibrate their presence and a unique ID code are getting a lot of attention right now, but they are not new. RFIDs are already being used in a number of ways. For example, the *key chains* issued by gasoline retailers that allow customers to pay for their purchases at the pump contain RFIDs. Now, retailers and governments are proposing to insert these tiny chips in everything from travel documents to paper currency and even items of clothing. Since RFIDs can be read at a distance, this raises a number of privacy concerns.

A retailer may be able to identify you when you walk into the store wearing an RFID-chipped garment. A government may one day be able to monitor the movements of visitors after they enter the country.

Spyware, a new surveillance technology, has replaced “cookies” as the latest Internet privacy villain. Spyware is software that surreptitiously installs itself on your computer and then secretly forwards information about your online activities without your permission or even knowledge. Because spyware can arrive as part of an unsolicited e-mail, you may not know how the programs arrived onto your machine or how to remove them.

Protecting your privacy rights

While these technologies have received a great deal of attention over the past year, the privacy threats they pose can, for the most part, be addressed by applying fair information principles. These principles can be found in *Personal Information Protection and Electronic Documents Act (PIPEDA)* which guides how your personal information can be collected, used and disclosed.

Although there are various ways of expressing these fair information principles, they can be distilled to a few key points:

- Personal information should only be collected, used or disclosed with the individual's knowledge and consent;
- Organizations should only collect as much information as they need;
- Organizations should explain why they are collecting the information and the information should only be used for those purposes;
- Individuals should be able to correct or amend information about themselves; and
- Organizations should have policies and practices governing the collection, use and disclosure of personal information, including destruction policies and procedures to safeguard the information.

While there is no doubt these surveillance technologies have a great potential to invade our privacy and compromise our personal information, there are ways to mitigate their impact. A coalition of consumer privacy and civil liberties organizations has released a position paper on the responsible use of RFIDs; our Office is preparing guidelines on the use of video surveillance by law enforcement agencies; individuals can become more familiar with spyware to protect themselves.

Enhancing security: at what cost?

Ultimately, the enhanced security actions of governments worldwide can pose a more fundamental and troubling challenge to our fundamental rights, including our right to privacy. Recent attempts to make us safer and more secure, both from international terrorism and more traditional public safety threats, raise serious privacy concerns.

Governments throughout the world, including the Government of Canada, continue to introduce measures to increase security based on the premise that if law enforcement and national security agencies have access to enough personal information about all of us we will have a safer, more secure society. In December 2003, the Government of Canada created the Canada Border Services Agency (CBSA), bringing together the border security and intelligence functions of the Canada Customs and Revenue Agency, Citizenship and Immigration Canada and the Canadian Food Inspection Agency. CBSA, in turn, is part of the new Department of Public Safety and Emergency Preparedness, along with the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP).

In April 2004, the Government of Canada issued its first ever National Security Policy. Among other things, it proposed to create an “Integrated Threat Assessment Centre” to facilitate the collection and analysis of intelligence and other information. According to the policy document, this “will help to reduce the risk that information held by one part of Government will fail to be provided in a timely fashion to those who can utilize it.”

The Government of Canada has announced that it will start issuing passports with facial recognition biometric technology in 2005. Although it was never an official government proposal, at least one Cabinet Minister has advocated the introduction of a national identification card.

Redefining borders

A border has become more than simply a river or a line on a map and a series of physical checkpoints. Borders are becoming virtual, posing privacy concerns. As the creation of the CBSA suggests, much of the Government of Canada’s national security agenda is focussed on the border. The result is a new concept of what constitutes a border. In December 2001, Canada and the United States signed the “Smart Borders” Declaration. The National Security Policy talks about “building a 21st century border” and “developing a next generation smart borders agenda with the United States and Mexico.”

Decisions about who can enter our country or who might pose a threat to security are increasingly being made long before the individuals arrive in Canada. In many cities, travellers flying to the United States can clear United States Customs at a Canadian airport. In the case of cyber-threats, the traditional notion of a border is irrelevant—cyber-attacks can originate from anywhere in the world. Recognizing this, Canada’s new national security policy notes that “The Government will also convene a high-level

national task force, with public and private representation, to develop the National Cyber-security Strategy to reduce Canada's vulnerability to cyber-attacks and cyber-accidents."

National borders are becoming less important. The border security policy of the United States is based on the creation of a buffer zone or a "cordon sanitaire" around North America – increasingly, Canadian policies are following suit. Our border security is becoming integrated with U.S. border security. Canada and the United States have created several integrated border enforcement teams. We share watch lists and the Government of Canada has been under pressure to share information with the U.S. government about all people travelling to Canada from abroad.

Smart borders or virtual borders require the collection of personal information—large amounts of personal information. This information is used to verify identity and to determine who should be allowed to enter the country without scrutiny, who needs to be watched and who should be refused entry. This is most evident from looking at various initiatives that have been implemented or proposed in the United States—the Total Information Awareness initiative (renamed Terrorism Information Awareness), the Computer Assisted Passenger Prescreening System (CAPPS II) which has since been abandoned due to privacy concerns, and the US-VISIT program. The Terrorism Information Awareness system is designed to integrate commercial and government databases – allowing access to credit card purchases, travel reservations, telephone records, e-mail records, medical histories, financial information – even public library use.

This emphasis on the collection of large amounts of personal information is also being seen in Canadian initiatives. CBSA is now collecting personal information about all airline passengers arriving in Canada—the Advanced Passenger Information/Passenger Name Record (API/PNR) initiative discussed in previous Annual Reports. Personal information is used in the NEXUS and FAST border-crossing programs to allow pre-approved low-risk travellers and commercial shipments to move back and forth between Canada and the United States.

More information = more security?

Much of the anti-terrorism legislation passed in Canada and abroad is based on the premise that the more information governments have about everyone, regardless of whether they have done anything to incur suspicion, the safer we will be.

We are told that collecting and using this information to identify threats is the price we have to pay to avoid racial and ethnic profiling and a reliance on stereotypes. Risk assessment tools, we are assured, do not recognize colour or religion, they simply analyze information.

As law enforcement and national security organizations collect more information, from more sources, about more individuals, and use that information to identify possible threats, there is an increasing possibility that people will be subjected to unnecessary scrutiny, that people will be wrongly singled out, and that people will be treated unfairly. Mistakes have occurred and will continue to occur. And because of a lack of transparency, we may never know why these individuals were wrongly targeted or where the system broke down.

The Office of the Privacy Commissioner does not think that we should have to choose between two bad options. There has to be a middle ground between racial profiling and collecting more information on everyone and subjecting everyone to increased scrutiny. Our Office is not convinced that reducing the freedoms of all individuals in society will prevent further threats to public safety by terrorists.

Our Office is not opposed to improving security. The question is how to do it in a way that does not destroy the fundamental values of our society. We are not opposed to the sharing of information among agencies, provided there are procedures and policies in place to protect this information, to ensure it is only used or disclosed for specific stated purposes which are reasonable, retained no longer than necessary.

Part of the answer to increasing security may lie in using the information we already have more effectively rather than collecting more information. This message came through very clearly in the Auditor General's March 2004 Report. That Report cites several situations in which Canadian agencies and departments failed to share or use existing information that would have enhanced security. The Report notes, for example, that although more than 25,000 Canadian passports are lost or stolen every year, officials at our borders are not equipped with lists of these lost and stolen documents.

Another troubling feature of the national security measures that are being introduced is the involvement of the private sector. Traditionally, national security has been carried out by government agencies relying primarily on intelligence information collected by these agencies. Increasingly, national security agencies are using personal information collected from individuals by the private sector for purposes unrelated to national security. This data is added to existing intelligence information and private sector expertise is being relied upon to develop the necessary analytical tools.

This raises a number of troubling questions. One set of concerns has surfaced in British Columbia as a result of the proposal that a Canadian subsidiary of an American company take over administration of the province's Medical Services Plan and PharmaCare programs. Critics of this proposal worry that this could potentially allow American

agencies such as the Federal Bureau of Investigation to obtain personal information about Canadians from U.S. companies under the *USA PATRIOT Act*. David Loukidelis, the British Columbia Information and Privacy Commissioner, has launched a public consultation process to examine the issue. Our Office submitted a position paper on the *USA PATRIOT Act* in the context of these public consultations.

Various anti-terrorism measures in the United States involve using private sector databases to confirm identity or to detect patterns of behaviour that might indicate someone poses a threat. Many of these initiatives, such as the Terrorism Information Awareness program, involve “data mining” — the use of database technology and sophisticated algorithms to sift through masses of information in an attempt to find hidden patterns and connections.

The Public Safety Act

This blurring of the line between government and the private sector can also be seen in Canada, most notably in the recently passed Bill C-7, the *Public Safety Act*.

Bill C-7 was a highly controversial piece of legislation that took two and a half years and four attempts to pass.

In March 2004, the current Commissioner appeared before the Senate Standing Committee on Transportation and Communications to comment on Bill C-7. Our comments focussed on two aspects of the bill: the amendments to the *Aeronautics Act* authorizing the Commissioner of the RCMP and the Director of CSIS to require air carriers and operators of aviation reservation systems to provide them with information about passengers; and a provision amending *The Personal Information Protection and Electronic Documents Act (PIPEDA)* to allow organizations to collect personal information, without consent, for the purposes of disclosing this information to government, law enforcement and national security agencies.

The RCMP and CSIS will use this passenger information to identify individuals who might pose a threat in terms of transportation safety and national security—purposes directly related to the legislation. However, the information can also be used for the enforcement of arrest warrants for offences punishable by five years or more of imprisonment—a purpose that has no direct connection to the legislation.

The amendment to *PIPEDA* is even more troubling because its implications are potentially far greater. Allowing private sector organizations to collect personal information without

consent for the sole purpose of disclosing this information to government, law enforcement and national security agencies effectively permits these organizations to act as agents of the state. It is one thing to allow an organization to disclose information already in its possession to government agencies without consent; it is quite another to allow – indeed to encourage — a private sector organization to collect this information without consent and then disclose it without consent. The amendment applies to any organization subject to *PIPEDA*, not just air carriers, it does not limit the amount of information that can be collected without consent, and it does not place any limits on the sources of information.

These provisions dangerously blur the line between the private sector and government by enlisting businesses, not only in the fight against terrorism, but in conventional law enforcement.

Despite our opposition, the opposition of several of our provincial and territorial colleagues and the opposition of a large number of other organizations, the Senate passed C-7 and the *Public Safety Act* received Royal Assent in May 2004.

“For every action...”

But for all the challenges this year, we also had reason for cautious optimism. If the threats to our privacy are increasing so too is the interest in defending our privacy.

If we are hearing more about RFIDs, cell phone cameras, event data recorders in cars and video surveillance cameras, it is because the office of the Privacy Commissioner, civil liberties groups, privacy advocates and others charged with protecting privacy are voicing these concerns. And the media are writing about these technologies because they know that the public is interested in privacy.

Opposition from U.S. privacy advocates, the media and politicians from both parties has forced the American government to abandon, scale back or delay a number of anti-terrorism measures. Operation TIPS, a program intended to enlist workers such as cable installers and parcel delivery employees to report suspicious activity was abandoned. The Total Information Awareness Project, which would have allowed the government to utilize “data-mining” to aggregate and analyze public and private commercial database information to track potential terrorists and criminals, never got off the ground. The Computer Assisted Passenger Prescreening System (CAPPS II) program that was supposed to identify foreign terrorists or persons with terrorist connections was abandoned due to privacy concerns.

In Canada, vocal public opposition to a national identification card has, at least for the moment, pushed this proposal onto the back burner. The Office of the Privacy Commissioner of Canada raised serious objections to this idea and we remain opposed.

In September 2003, Robert Marleau, the Interim Privacy Commissioner, appeared before the Standing Committee on Citizenship and Immigration to discuss our Office's opposition to a national identification card. Denis Coderre, the then Minister of Citizenship and Immigration, argued that a national identification card would provide a more secure and reliable proof of identity, help combat identity theft, make it easier for Canadians to travel abroad, and prevent racial profiling at the border.

The Interim Commissioner urged the Committee to reject the proposal on the grounds that:

"The privacy risks associated with a national identification card are substantial. The challenges of putting in place a national identification system that is workable, affordable, and respectful of the privacy rights of Canadians are enormous. A strong case for the benefits has not been made; to the extent that benefits would exist, they would be marginal at best."

More than 60 witnesses appeared before the Committee. Almost all opposed the introduction of a national identity card. Privacy and human rights groups, consumer lobby groups, religious and ethnic organizations, and major newspapers across the country have also opposed the concept.

We have also seen progress in terms of legislated efforts to protect privacy. We now have an official in every province and territory with a mandate to protect personal information contained in government records. Three provinces—Alberta, Saskatchewan and Manitoba—have laws specifically dealing with the protection of personal health information. Ontario has just passed similar legislation that is scheduled to come into force later in 2004. Quebec, Alberta and British Columbia now have laws in force governing the collection, use and disclosure of personal information in the private sector.

Ultimately the decisions we make now about privacy and whether or not we truly value it will shape the kind of society our children will inherit in the future. As an agency charged with protecting privacy, we must confront those who would trade away individual rights, for the promise of national security or privacy invasive technologies. We must ensure that the high value Canadians place on their privacy rights, is not lost or submerged in the chorus of voices calling for more security, and more information about all of us and work together in the future to meet the challenges that are surely coming our way.

POLICY PERSPECTIVE

One of the key roles of the Office of the Privacy Commissioner is to identify and analyze emerging privacy issues, and develop policies and positions that address them to advance the protection of privacy rights. Our research and analysis of important issues stimulates and informs public debate, engages Canadians and raises awareness. This enables our Office to serve as Parliament's window on privacy issues and to provide timely and knowledgeable advice on the impacts of legislative and regulatory initiatives, and to apprise the public of risks to privacy and ways to respond to them.

Our Office has undertaken a concerted effort to strengthen our relations with Parliament and to better serve its needs. To this end, we have created a new Parliamentary Liaison function specifically dedicated to briefing Members of Parliament and Senators on specific privacy issues, monitoring legislative and regulatory initiatives, and arranging for the Commissioner and senior staff to provide informed advice to Parliamentarians on the privacy implications of emerging law and policy.

In the 2003-2004 reporting period, the Office effectively advocated for the protection of privacy rights on a range of social, technological, and political issues including:

- Identity cards
- Surveillance technologies and video surveillance
- Governmental access to commercial holdings of personal information
- The privacy of personal health information
- Regulating privacy in a federal system

Identity cards

Identity cards have been a long-standing concern for our Office and for privacy and data protection commissioners worldwide. An identity card, and the identity system in which it is embedded, is not simply a convenient tool to confirm the identity of an individual. It is also an information management tool to access, combine, and manipulate personal information. A single card, used as an identifier in a wide variety of transactions with government and the private sector, can be a powerful means of amassing and mining information about an individual, and ultimately tracking and monitoring the individual. It is this power that makes identity cards a threat to privacy.

OPC Position

The Office raised serious objections when the Minister of Citizenship and Immigration proposed a debate on the subject of a national identity card in the fall of 2003.

Our efforts resulted in positive coverage and a number of editorials and columns in major newspapers rallying behind our views on the issues, including an editorial by the *Globe and Mail* on September 22, 2003, commending Interim Privacy Commissioner Robert Marleau's "cogent, thoughtful analysis," of the issue presented to the House Standing Committee on Citizenship and Immigration. Our presentation raised a number of questions, including the considerable risks and costs of setting up a national identification system, and the significant challenge of making it practical, affordable, and respectful of privacy. The advantages of such a system were, in his view, marginal, and overwhelmed by the cost to privacy.

The Office continues to hold this view, and while the proposal for a national identity card appears for the time being to be on the back burner, we remain vigilant.

Surveillance technologies

Technology can threaten privacy and is a growing preoccupation of privacy advocates and privacy commissioners. This is particularly true when increasingly powerful technologies for observing and recording information about people's location, movements, behaviour, and actions are combined with increasingly powerful computers for storing, sorting, mining, and analyzing this information. Think, for instance, of the information that could be collected about you if you drove to a store in your Global Positioning System (GPS) equipped car, used your credit card to pay for a buggy-full of goods individually identifiable by their radio frequency identification tags ("RFIDs"), in a store using video cameras equipped with facial recognition technology. Now imagine all that information about you linked together by a computer, linked with all the other data from your credit card, black box, GPS, RFIDs, and exposure to video cameras, and analyzed for patterns. The example is hypothetical, but it is by no means inconceivable.

OPC Position

This challenge has led the Office to focus on strengthening its capacities for understanding and dealing with new technologies. The Office has also launched a Privacy Lecture series which has brought a number of distinguished guests to speak to staff and interested members of the community on issues of technological change and policy responses. The Office also recently launched a Contributions Program to encourage research projects that focus on the intersection of privacy and technology.

We recognize, however, that the problem is not technology itself, but the failure to control its uses properly. Our basic position with respect to these technologies is that at a minimum their use must be governed by the principles of fair information practices. This approach applies to technologies as varied as smart cards, event data recorders (“black boxes”) and RFIDs. People should be told what information is being collected about them, by whom, for what purposes; they should be told what is being done with it and who it is being disclosed to; they should be able to control the collection, use and disclosure of the information through the power of granting or withholding consent; the information should be securely held and treated as confidential; people should have a right of access to their information, and a right to correct it where necessary.

When technologies are used for surveillance, they are subject to an even higher standard. Their deployment and use should be limited to special circumstances where they are justified as a proportionate response to a pressing and substantial problem. Claims that they are justified should be subject to close scrutiny and stringent tests.

Video surveillance

Video surveillance is perhaps the best-known and most obvious example of surveillance technologies. Some people have difficulty articulating or even understanding how they might have a sense of “privacy” in the middle of a public park or walking on a city street, surrounded by other people, and fully visible and audible to them. Yet few people have difficulty understanding that there is something wrong with cameras watching them, perhaps recording their actions, perhaps focusing on them in minute detail, whenever and wherever they go in public. We have not reached that point in Canada – not like the U.K., with its estimated 4 million cameras, one for every 14 residents. But in the course of a typical day, we are repeatedly caught on camera in banks, shopping malls, parking garages, staircases, convenience stores, and, increasingly, in public places such as parks or city streets.

OPC Position

Our Office and most privacy commissioners and privacy advocates are in agreement that video surveillance presents a grave challenge to privacy. It subjects everyone to the scrutiny of police or other authorities, regardless of whether they have done anything to arouse suspicion. At the very least it circumscribes, if it does not eradicate outright, the “shell” of privacy and anonymity that we are entitled to as we go about our law-abiding business. There are good reasons to suspect that video surveillance has a chilling effect on behaviour.

In 2001, the Office investigated a complaint regarding the RCMP's video surveillance of a public park in Kelowna. The conclusion of the investigation was that this surveillance was not justified. This led to protracted discussions with the RCMP, which insisted on continuing the system, although it did agree to stop recording and use the system simply for monitoring. An attempt to have the question addressed in court became mired in procedural issues, and in July 2003 the Office took the decision to withdraw the case. Meanwhile, municipal police forces in a significant number of major Canadian cities indicated an interest in installing public video surveillance systems, and in some cases moved forward with them.

Shortly after taking office, the current Commissioner decided on an enhanced approach to this issue, and developed guidelines for the use of video surveillance by public authorities. These guidelines set out principles for evaluating the necessity of resorting to video surveillance and for ensuring that, if it is conducted, it is done so in a way that minimizes the impact on privacy. So, for example, video surveillance should only be a response to a real and pressing problem, where less-privacy invasive methods will not suffice; video surveillance systems should be designed to have the least possible impact on privacy, running for limited periods and avoiding capturing images of areas such as office or apartment interiors where people have an even greater expectation of privacy.

Government access to commercial holdings of personal information

Another matter of concern to our Office, privacy advocates and commissioners is access by law enforcement and national security agencies to personal information collected by private sector organizations. Many people object to the private sector collecting information about them specifically because they worry about it finding its way into governmental hands.

There can be times when this collection is legitimate, but without controls and oversight, it can tip over into what is in effect deputizing private sector organizations as law enforcement agents, and commandeering personal information that they have collected from individuals for entirely different reasons, in violation of the most basic fair information practices.

OPC Position

The Office's concern about this came to a head in 2003 over the issue of the requirements for airlines to disclose personal information about passengers – including their itinerary, companions, method of payment for tickets, contact addresses and telephone numbers, and even dietary and health-related requirements – to what was

then the Canada Customs and Revenue Agency, so that customs and immigration agents could assess security risks that they might present. While that specific issue was partially resolved with a compromise agreed to between our Office and the CCRA, the larger issue of access by security agencies to the personal information of passengers is still present.

The *Public Safety Act, 2002* which received Royal Assent on May 6, 2004, (shortly after the end of our reporting period) allows the RCMP and CSIS to use passenger information provided by air carriers and operators of aviation reservation systems to identify not just individuals who might pose a threat to transportation safety and national security, but any individual named in an arrest warrant for an offence punishable by five years or more of imprisonment. Moreover, the *Act* amends *PIPEDA* to allow private sector organizations to collect personal information, without consent, for the purposes of disclosing this information to government, law enforcement and national security agencies – effectively permitting these organizations to act as agents of the state, and not only in the fight against terrorism, but in conventional law enforcement.

It was for this reason that the current Commissioner appeared in March 2004 before the Senate Committee charged with examining the proposed law, and raised her concerns. Although Parliament chose to pass the law in spite of opposition from our Office and other privacy advocates, it has not lessened our concern about the issue.

The privacy of personal health information

The application of *PIPEDA* to personal health information is something that was troubling to many in the health care sector even before *PIPEDA* was passed, and it was partly in the interest of resolving uncertainties around the issue that Parliament chose to exempt personal health information from the coverage of the *Act* for the first year after it was passed.

By 2003, various health care sector groups, along with provincial and territorial ministries of health, were looking with increasing apprehension at the looming January 2004 expansion of *PIPEDA*'s scope to all commercial activity. They expressed renewed concern about the impact of the *Act* on the health care sector, and some parties formally asked for an amendment to the *Act* to either “carve out” health information from it or delay the scheduled next phase of its implementation.

Physician's offices, and the offices of other health care providers such as dentists and chiropractors, are engaged in commercial activity. Thus, the personal information that they

collect, use and disclose is subject to *PIPEDA*. The *Act* does not extend to the core activities of hospitals – that is, patient care. This is clearly something within the jurisdiction of the provinces (although *PIPEDA* would apply to clearly commercial peripheral activities, such as a parking lot operated by the hospital if it collected personal information).

OPC Position

The Office's position is that *PIPEDA* is a quite workable instrument to protect personal health information, without imposing an unreasonable burden on health care providers. Overall, the traditional doctor-patient relationship will not have to change significantly. While patient consent to the collection, use, and disclosure of their personal information has to be based on knowledge, this does not mean that doctors must hold conversations with every patient. Patient understanding can be achieved through notices, posters, brochures, and information on the forms people typically fill out when providing a medical history.

Moreover, there are many uses or disclosures that a patient would reasonably expect for care and treatment – for example, disclosures from a general practitioner to a specialist or laboratory, or between a physician and a pharmacist in discussing a prescription. For these reasonably expected uses and disclosures of a patient's personal information, health care providers can rely on implied consent, as long as it is based on a general understanding of how personal information will be used and disclosed. More explicit consent would be necessary for uses or disclosures that a patient would not reasonably expect. The disclosure of information for research purposes is one such example.

In order to address concerns, and to promote this common-sense view of the way *PIPEDA* will work, our Office has joined Health Canada, Industry Canada, and the Department of Justice Canada in an interdepartmental working group to develop communications tools and guidance, respond to questions, and to meet with health care associations to address their concerns and explain our position.

We have noted that not all of the health care sector foresees significant problems complying with *PIPEDA*. For example, the Royal College of Dental Surgeons of Ontario has developed an excellent compliance package that it has distributed to every dentist's office in Ontario.

Regulating privacy in a Federal system

In a modern economy, where personal information flows back and forth across territorial boundaries – where, for example, information about customers in Madrid of a company based in Montreal can be processed in Berlin and stored in Vancouver – privacy protection

has to be seamless and harmonized. Individuals need protection of their personal data, and rights with respect to it, regardless of what jurisdiction it travels to.

That is a complicated task internationally, one that requires constant negotiation and adjustment. But even when the personal information never leaves the country it is a challenge in a federal system like Canada's, with its varying jurisdictional responsibilities. The year in review marked a number of important developments in the movement towards full, harmonized privacy protection in Canada.

In October, 2003, the B.C. government passed its *Personal Information Protection Act* to apply to private sector commercial activity. Alberta followed in December, 2003, with an identically-named and very similar statute. On January 1, 2004, *PIPEDA* came fully into effect, extending to cover commercial activities throughout Canada except where substantially similar provincial legislation applies. Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* had already been declared substantially similar by the Governor in Council in November 2003; as we go to print, similar declarations are expected with respect to the B.C. and Alberta laws.

OPC Position

The "substantially similar" provision in *PIPEDA* ensures consistent levels of privacy protection in all sectors of the economy throughout the country, but it does not make problems magically vanish. Harmonized privacy protection has its own special challenges.

Conscious of this, federal and provincial privacy commissioners and staff have worked together to help businesses understand which law applies to them, and helped individuals understand their rights, and how to seek redress under the appropriate law. The Offices of the B.C. and Alberta Information and Privacy Commissioners have jointly released a guide (available on their websites, and linked to from ours) to help businesses and individuals sort through what can be an initially confusing picture. This complements the work done by our Office in making available various materials, such as a video streaming speech by the Commissioner, and an E-kit for businesses, that help to ease the implementation of *PIPEDA*.

In an increasingly connected and technologically sophisticated world, potential new threats to the privacy of our personal information seem to arise daily – if not by the minute. As we look ahead, our Office is dedicated to fostering a clear understanding of emerging privacy issues for Parliamentarians, the public and lawmakers, and to continue providing a cogent analysis of national and international privacy risks and challenges as they evolve.

SUBSTANTIALLY SIMILAR PROVINCIAL LEGISLATION

Under the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, the Governor in Council can issue an Order exempting an organization, a class of organizations, an activity or a class of activities from the application of *PIPEDA* with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation that is substantially similar to *PIPEDA*.

The intent of this provision is to allow provinces and territories to regulate the personal information management practices of organizations operating within their borders, provided that they have passed a law that is substantially similar to *PIPEDA*.

If an Order is issued, *PIPEDA* will not apply to the collection, use or disclosure of personal information by organizations subject to the provincial act. Personal information that flows across provincial or national borders will continue to be subject to *PIPEDA* and the *Act* will continue to apply within a province to the activities of federal works, undertakings and businesses that are under federal jurisdiction such as banks, airlines, and broadcasting and telecommunications companies.

Process for assessing provincial and territorial legislation

On September 22, 2001, Industry Canada published a notice setting out the process that the department will follow for determining whether provincial/territorial legislation will be deemed substantially similar.

The process will be triggered by a province, territory or organization advising the Minister of Industry of legislation that they believe is substantially similar to *PIPEDA*. The Minister may also act on his or her own initiative and recommend to the Governor in Council that provincial or territorial legislation be designated as substantially similar.

The Minister has stated that he will seek the Privacy Commissioner's views on whether or not legislation is substantially similar and include the Commissioner's views in the submission to the Governor in Council. The process also provides for an opportunity for the public and interested parties to comment on the legislation in question.

According to the Canada Gazette notice, the Minister will expect substantially similar provincial or territorial legislation to:

- incorporate the ten principles in Schedule 1 of the *PIPEDA*;
- provide for an independent and effective oversight and redress mechanism with powers to investigate; and
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

Provincial and territorial legislation passed to date

The Office of the Privacy Commissioner is required by subsection 25(1) of *PIPEDA* to report annually to the Parliament of Canada on the “extent to which the provinces have enacted legislation that is substantially similar” to the *Act*.

Quebec’s *An Act Respecting the Protection of Personal Information in the Private Sector* came into effect, with a few exceptions, on January 1, 1994. The legislation sets out detailed provisions that enlarge upon and give effect to the information privacy rights in Articles 35 to 41 of the *Civil Code of Quebec*. In November 2003, the Governor in Council issued an Order in Council (P.C. 2003-1842, 19 November 2003) exempting organizations in that province, other than federal works, undertaking or businesses, from the application of *PIPEDA*.

In the spring of 2003, the provinces of British Columbia and Alberta introduced similar legislation, Bills 38 and Bill 44 respectively. The two Bills were passed by their respective legislatures and they both came into force on January 1, 2004.

The two laws — both called the *Personal Information Protection Act* — are similar to *PIPEDA*, but they are not identical. The application of the two provincial *Acts* is broader. Unlike *PIPEDA*, they apply to all organizations, with a few exceptions, not just those that are engaged in commercial activities. They also differ from *PIPEDA* in that they contain different rules for employee personal information than for other personal information. As well, the *Acts* give the two provincial commissioners authority to issue orders, for example, to require an organization to give an individual access to his or her personal information or to require an organization to cease collecting, using or disclosing certain personal information. By comparison, the Privacy Commissioner of Canada does not have order-making powers.

Using the criteria set out in the notice — the presence of the ten principles found in Schedule 1 of *PIPEDA*, independent oversight and redress and a provision restricting collection, use and disclosure to legitimate purposes (a reasonable person test) — we have concluded that, on balance, the British Columbia and Alberta *Acts* are substantially similar to *PIPEDA*.

The other legislative initiative of note was the introduction and passage of Ontario's Bill 31, the *Health Information Protection Act*. The *Act* received Royal Assent on May 20, 2004 and is scheduled to come into force on November 1, 2004. We are still reviewing the *Act* and we are not yet in a position to comment on whether or not we consider it to be substantially similar to *PIPEDA*.

PART ONE

Report on the *Privacy Act*

INTRODUCTION

The *Privacy Act* has been in force in Canada since 1983, protecting the personal information of individuals held by institutions of the federal government. The *Act* governs the collection, use, disclosure, retention and disposal of personal information by federal government departments and agencies. It gives individuals the right to request access to and correction of their government-held personal information. The *Act* also sets out the duties, responsibilities and mandate of the Privacy Commissioner of Canada.

The Commissioner receives and investigates complaints from individuals who believe their *Privacy Act* rights have been violated. The Commissioner may herself initiate a complaint and investigation in any situation where she has reasonable grounds to believe the *Act* has been violated.

The Privacy Commissioner of Canada works as an ombudsman to resolve complaints through mediation, negotiation, and persuasion whenever possible.

However, the *Act* gives the Commissioner broad investigative powers in order to carry out her mandate. She may subpoena witnesses, compel testimony, and enter premises to obtain documents or to conduct interviews. It is an offence under the *Act* to obstruct an investigation. The *Act* does not grant order-making powers to the Commissioner.

However, the Commissioner can and does make recommendations for changes in the information-handling practices of government institutions when necessary. The Commissioner may conduct audits of any federal department or agency at any time, and may recommend changes to any practices that are not in compliance with the *Privacy Act*.

The Commissioner is required to submit an Annual Report to Parliament, detailing the activities of the Office in the previous fiscal year. This Report covers the period from April 1, 2003 to March 31, 2004 for the *Privacy Act*.

INVESTIGATIONS AND INQUIRIES

The Office of the Privacy Commissioner is responsible for investigating complaints received from individuals under section 29 of the *Privacy Act* (and section 11 of the *Personal Information Protection and Electronic Documents Act*, known as *PIPEDA*)

Investigations serve to establish whether individuals have had their privacy rights violated and whether they have been accorded their rights of access to their personal information. Where privacy or access rights have been violated, the investigation process seeks to provide redress for individuals and prevent violations from reoccurring.

Last year the Office received 4,206 new complaints – an all-time record representing a 250 per cent increase over last year. There were several contributing factors:

- 472 members of Canada's aboriginal communities complained that they were required by Health Canada to sign a broadly worded consent form in order to receive government-funded health benefits;
- 608 correctional officers lodged more than 1,100 complaints against Correctional Service Canada (CSC) for refusing to give them copies of their employee personnel files;
- 107 employees at the Joyceville Institution complained that CSC failed to protect their personal information, after learning that a list containing their home addresses and phone numbers had been found amongst the inmate population; and,
- 38 offenders in British Columbia filed a total of 950 complaints against CSC for not providing timely responses to requests for their personal information held in the 25 standard personal information banks CSC maintains on offenders.

It was also a record year in terms of productivity with investigators concluding 3,315 complaints.

Complaints under the *Privacy Act*

It was also a record year in terms of productivity with investigators concluding 3134 complaints. Although we did close 3483 cases last year, 2323 of these represented investigative work done two years earlier. This year's statistics represent active investigative work completed in 2003/2004. They were concluded as follows:

Not well-founded	1,243
Well-founded	1,180
Well-founded/resolved	69
Resolved	11
Settled	265
Discontinued	366

Definitions of findings under the *Privacy Act*

Not Well-founded: This finding means that the investigation uncovered no or insufficient evidence to conclude that the government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: This finding means that the government institution failed to respect the *Privacy Act* rights of an individual.

Well-founded/Resolved: This finding means that the allegations are substantiated by the investigation, and the government institution has agreed to take corrective measures to rectify the problem.

Resolved: This finding is used for those complaints where *well-founded* would be too harsh to fit what essentially is a miscommunication or misunderstanding. It means that this Office, after a full and thorough investigation, has helped negotiate a solution that satisfies all parties.

Settled during the course of the investigation: This disposition is used when the Office has helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.

Discontinued: This means that the investigation was terminated before all the allegations were fully investigated. A case may be *discontinued* for any number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

Early resolution: This is a new type of disposition, which the Office will begin using in April 2004. It will be applied to situations where the issue is dealt with before a formal

investigation is undertaken. For example, if an individual lodges a complaint about an issue that the Office has already investigated and found to be compliant with the *Privacy Act*, we would explain this to the individual. We also receive complaints where proceeding with a formal investigation could have adverse implications for the individual, which are discussed at length with the individual. In these situations, where the individual chooses to not proceed further, the file is closed as “*early resolution*”.

Select cases under the *Privacy Act*

HEALTH CARE

Health Canada's Non-Insured Health Benefits Program

Overview

In the summer of 2003 the OPC received several hundred complaints, as well as numerous inquiries, about Health Canada's decision to require First Nations and Inuit recipients of certain government-funded health benefits to sign a consent form endorsing the department's practices with regard to the collection, use, and disclosure of their personal information. The complainants objected to the complex language of the form, its broad scope, and the lack of adequate measures to protect personal information held by third-party service providers.

Several aboriginal associations, including the Assembly of First Nations and the Inuit Tapiriit Kanatami, supported the complaints and made representations on behalf of their membership.

The impetus for the campaign was a recommendation from the Auditor General that Health Canada improve its tracking mechanisms to prevent the misuse of prescribed drugs. Health Canada also worked to respect the right of benefit recipients to be fully informed about the possible consequences of a drug utilization review.

The complainants felt that the program benefits were and had always been a matter of treaty rights, and that they had no real choice but to agree to review practices that Health Canada was now planning to impose or lose their benefit coverage. They objected to the complex language of the form, its broad scope, and the lack of adequate measures to protect personal information held by third-party providers.

Actions taken by the OPC

We accepted the complaints under the provisions of the *Privacy Act*, and subsequently determined that there was no infringement of a provision of that *Act*. However, our Office continued to work with the aboriginal associations and the department to craft a new approach to the consent initiative that would address privacy concerns. We jointly identified the critical points in the health benefits program requiring fully informed consent of recipients. In addition, we agreed that the privacy provisions of the contracts with third-party providers needed to be strengthened, and Health Canada committed to do so. We also agreed the language of the consent forms needed to be as simple and clear as possible.

Outcome of OPC Actions

Health Canada subsequently proposed an alternative approach to the consent initiative, one that has been supported by aboriginal stakeholders. The approach is as follows:

- the department will continue to promote consent as a matter of best practice (a position that our Office endorses), but will no longer require that everyone sign a form;
- it will implement a mechanism to obtain the express consent of benefit recipients where there are patient safety issues or concerns that the program is being used inappropriately;
- it has established a Health Canada/ First Nations Drug Utilization Review Committee, composed of licensed health care professionals, experts in drug use evaluation, Aboriginal health issues and drug utilization;
- it is developing a Privacy Code that sets out the program's collection, use and disclosure practices. The Code meets the higher standard of consent embedded in the *Personal Information Protection and Electronic Documents Act*, as many of the third-party providers associated with Health Canada's program are subject to that *Act*.

Our Office has offered continuing support to achieve an appropriate balance between the privacy interests of benefit recipients, and the program imperatives of Health Canada.

RCMP medical questionnaire too intrusive for civilian applicants

Overview

A woman was denied a civilian telecommunications officer position with the RCMP after refusing to answer certain questions posed on a medical history questionnaire she was asked to complete during the recruitment process. The questions included:

- *“Do you have monthly menstrual periods?”*
- *“What was the date of your last period?”*
- *“Are your menstrual periods painful?”*
- *“When was your last Pap smear test?”*
- *“How many times, including abortion and miscarriage have you been pregnant?”*

Candidates were also asked if they had varicose veins, arthritis, phlebitis, hay fever, venereal disease, and whether any of their family members had diabetes, cancer, high blood pressure, tuberculosis or heart disease.

Actions taken by the OPC

We established that the woman was required to submit to the same testing process as a candidate applying to be a police officer. The RCMP, however, could not demonstrate how such questions were relevant to a civilian desk job. We concluded that the complaint was well-founded.

Outcome of OPC Actions

Following discussions with the RCMP, its Health Services officials agreed to suspend the use of this questionnaire for civilian candidates. It has undertaken to create a new form specifically for telecommunications officer candidates and geared to the medical requirements of the job, such as hearing, upper body movement, and diseases that could affect cognitive thinking and speech recognition.

While the woman also objected to having to undergo a psychological assessment, the RCMP explained to our satisfaction that telecommunications officers are often the only lifeline between victims and the police officers handling emergency calls. The RCMP therefore needs to ensure that candidates are able to withstand the pressures of the job and deal comfortably with the situations they encounter. Collection of personal information to assess candidates' ability to deal with those stresses is therefore reasonable and appropriate.

SURVEILLANCE TECHNOLOGIES

Video surveillance cameras at Nanaimo Harbour Front scaled back

Overview

A British Columbia resident, aware of the former Commissioner's position on video surveillance on the streets of Kelowna, lodged a complaint about the Nanaimo Port Authority's plans to install video surveillance cameras within its Harbour Front.

The Port Authority provides, among other things, mooring facilities for a fee. The customers paying for this service expect the Port Authority to protect their property. Several customer complaints about vandalism and thefts from vessels prompted the Port Authority to consider installing cameras on its piers. Other areas of the property were also earmarked for surveillance – the Port Authority's offices, the parking lots, a boardwalk, the laundry facilities, and the area where fishers and other boat owners deposit pollutants from their vessels that could endanger the environment.

Actions taken by the OPC

While we did not object to the cameras installed in most of these areas for security purposes, we had concerns about monitoring activities along the publicly accessible boardwalk.

Outcome of OPC Actions

The Port Authority's officials readily agreed to move the cameras away from that area. It also agreed to post signs alerting the public of the presence of surveillance cameras at the Harbour Front.

The investigation helped the Port Authority put safeguards in place to ensure that data collected by the cameras is adequately protected, that it is retained no longer than necessary, and that access and disclosure of the information is closely restricted. Given the Port Authority's willingness to address our concerns, the complaint was deemed resolved.

A different kind of fishing expedition?

Overview

The Office received two complaints about the Fisheries and Oceans Canada Observer Program that requires fishers as a condition of their licence, to allow an observer to stay

on board their commercial fishing vessels, including during the evening and overnight hours, and during non-fishing hours. Some fishers have only family members on board, and their vessels are too small to accommodate a stranger. One of the complaints also concerned the intrusiveness of an alternative to having the observer on board – electronic monitoring by use of video cameras and global positioning systems.

Actions taken by the OPC

The investigation established that the Observer Program is authorized by regulation. Observers' duties are to monitor fishing activities by, among other things, examining and measuring fishing gear, verifying the weight and species of fish caught, inspecting fishing records and conducting biological samplings of fish. The only personal information observers would normally collect include the names, addresses and contact numbers of vessel personnel. All of the remaining information collected relates to the fishing activities under observation.

While having a stranger on board vessels is intrusive by nature, the issue is one of "personal" privacy, which does not fall under the *Privacy Act*, rather than one of protection of personal information.

Outcome of OPC Actions

The Office concluded the complaints were not well-founded. Although the complaints were not well-founded, we discussed the complainants' concerns with Fisheries and Oceans Canada officials who maintained that the department must retain the ability to monitor the fishery. However, they agreed to consult the fishing industry, and we encouraged them to recommend other less intrusive options to carry out this program activity.

HANDLING OF PERSONAL INFORMATION

Where were you born?

Overview

An individual complained that the practice of the Department of Foreign Affairs and International Trade of displaying a passport holder's place of birth on the passport was discriminatory and violated individual privacy.

Actions taken by the OPC

Our investigation determined that more than 85 countries require that the place of birth be indicated on the passport before entry is permitted. Foreign Affairs officials

indicated that when negotiating reciprocal visa-waiving agreements, the place of birth on the passport is often a condition stipulated by other countries. The International Civil Aviation Organization also recommends including place of birth on travel documents.

Nevertheless, passport holders have had the option of having this information displayed or not since 1986. Those choosing to have it excluded must sign statements that they were informed they might encounter difficulties at border points, such as additional questioning by customs officers, the requirement to obtain a visa, or even denial of entry.

Outcome of OPC Actions

We concluded that the complaint was not well-founded.

Correspondence to CRTC posted on Web site

Overview

An individual wrote to the Canadian Radio-television & Telecommunications Commission (CRTC) supporting the licence application of a cultural broadcasting company.

The CRTC posted the individual's correspondence on its Web site exactly as it had been received, including her name, address, phone number and e-mail address. This practice is explained on the Web site, but unfortunately the individual had not noticed this and had no idea that her correspondence would be published in this fashion. She was also not aware that she could ask the CRTC to remove personal identifiers before the correspondence was posted.

When the individual learned that her personal information was on the Web site, she immediately asked that it be removed. The CRTC complied within 48 hours. However, in the meantime, the search engine Google (and possibly others) had picked up the data. When the individual's name was "Googled," her original correspondence to the CRTC would come up.

The individual contacted Google requesting that it too remove her personal information. It replied that it would not do so without a formal request from the webmaster of the site that originally posted the information on the Internet. The individual forwarded her correspondence to the CRTC for appropriate follow-up action, but her personal information remained on the Internet.

Actions taken by the OPC

Following our Office's intervention, the CRTC's webmaster made three requests to Google. None of these requests received a formal response. However, Google did eventually remove the individual's personal information – to her relief and satisfaction.

Outcome of OPC Actions

We closed the file as “settled during the course of investigation.”

Taxpayers must comply with Canada Revenue Agency demands for information

Overview – Case One

Two cases the Office investigated last year illustrate the Canada Revenue Agency's (CRA's) authority to require taxpayers to provide very private information.

In the first case, during a routine audit of an Ontario man's 2001 tax return, the CRA asked him to provide a copy of the separation agreement with his former spouse to substantiate the amounts he claimed as child support payments. Although he agreed to provide those portions of the separation agreement that dealt specifically with the payments, he objected to the CRA's insistence that it be given a complete unsevered copy.

Overview – Case Two

In the second case, a Quebec woman complained about the detailed questions posed by a CRA officer attempting to collect an outstanding tax debt. She had been unable to pay the full amount of her tax debt within a reasonable period and requested an extended payment arrangement.

Actions taken by the OPC

Following our investigation of the first case, we explained to the complainant that the CRA had the legal authority under the *Income Tax Act* to demand this information in order to satisfy itself that there were no other clauses in the agreement about child support that might have an impact on his tax situation.

In the second case, we determined that the CRA tries in such cases to reach a mutually acceptable payment schedule with tax debtors based on their financial situation. This requires the individual to make full disclosure of his/her income and his/her monthly expenses as well as assets and liabilities. If an acceptable arrangement is not reached, the CRA may take legal action to recover the debt, including seizing and selling the debtor's assets.

Outcome of OPC Actions

In the first case, in an effort to limit the privacy intrusion, the CRA agreed to keep for its records only those portions of the agreement pertinent to the man's child support payments that it needed to determine his entitlements. The man was pleased with the compromise, and the case was closed as "settled during the course of investigation."

In the case at hand, the CRA officer questioned the woman's expenses for costly prescription drugs to deal with her medical condition, which she claimed precluded her from making significant advances in reducing the debt. The officer asked the woman to obtain a note from her treating physician confirming her condition, which would be factored into the CRA's assessment of her monthly expenses. The complainant accepted our explanations about the CRA's rationale for such an unusual request and the implications should she not comply. The file was closed as "settled during the course of investigation."

Incidents under the *Privacy Act*

Incidents of mismanagement of personal information that warrant further review are brought to the attention of our Office. We conducted 30 such reviews last year. Of note, seven of the incidents related to clients of government departments receiving another client's personal information in error.

Health Identification Cards forwarded to wrong address

In one such case, Veterans Affairs Canada (VAC) was in the process of re-issuing approximately 143,000 client health identification cards with a new National Contact Centre toll-free number. A corrupted data file used during production assigned to about 12,000 clients in Ontario contained the addresses of other clients and before the error was detected, the new cards were incorrectly forwarded to the wrong addresses. VAC officials told us that as soon as they learned about the problem, they immediately halted production until enhanced quality control procedures were implemented. The department contacted all the clients affected by the error.

Misdirected passports

The Office also reviewed two instances of misdirected passports. In one case, an Alberta man received an envelope from the Passport Office containing the passport, birth certificate, credit card information and driver's licence of a woman from Quebec, along with his own documents. In the second case, a Canadian citizen living in Colorado, USA, was mistakenly sent the passport, green card, birth certificate and credit card number

belonging to woman living in Wisconsin, USA. The Wisconsin resident received the documents belonging to the Colorado woman. We determined that human error was the contributing factor in both cases; the passports were prepared and mailed on the same day, along with several thousand others.

With that many mailings in one day, mistakes in stuffing envelopes can happen. The Passport Office indicated that in the six-month time frame between incidents, it had processed in excess of 500,000 applications. The increased volume was a result of additional security procedures and travel restrictions put in place internationally after the events of 9/11. Since enhancements to the mailing procedures were implemented in January 2004, neither the Passport Office nor this Office has received further complaints about misdirected passport documentation.

Stolen computers raise privacy concerns

In another case, six computers were stolen from the CRA's Laval, Quebec tax services office. One of the computers was being used to test computer applications. It was password protected, and contained approximately two million records from four confidential databases. These databases contained personal information, but not tax return information. More than 120,000 affected individuals were advised of the security breach, and given tips on what to do to reduce the possibility of identity theft, such as:

- review and verify all bank account, credit card and other financial transaction statements;
- report any problems/delays with mail delivery to Canada Post;
- report to Human Resources and Skills Development Canada any suspicion about use of the social insurance number (SIN); and
- contact a credit reporting agency such as Equifax or Trans-Union, which are experienced in helping individuals in such matters.

Sixteen individuals later lodged formal complaints with our Office, alleging that the CRA had not adequately protected their information. The CRA indicated that as a result of a lapse in security procedures, the computer had not been stored in a secure room at the end of the day. Appropriate disciplinary action, consistent with CRA policies, was taken.

Public interest disclosures under the *Privacy Act*

Paragraph 8(2)(m) of the *Privacy Act* gives heads of government institutions the discretion to disclose personal information without the individual's consent where the disclosure

would benefit the individual or where there is a compelling public interest that outweighs the invasion of the individual's privacy. Under subsection 8(5), the head of the institution is required to notify the Privacy Commissioner of such disclosures, preferably in advance unless there is some urgency that dictates otherwise.

Last year we received 67 such notices. Correctional Service Canada (CSC) topped the list with 20 notices, most of them related to the disclosure of personal information about offenders who died in custody. CSC routinely relies on the public interest provisions of the *Privacy Act* to share information with family members wanting access to the reports prepared by CSC staff who reviewed the circumstances surrounding the offender's death.

The RCMP sent 15 notices of impending public interest disclosures. Most of these concerned individuals released from custody at the end of their sentences who were considered at high risk to re-offend. The RCMP intended to issue press releases in communities where the offender planned to live to alert residents of the individual's presence and of specific conditions attached to the individual's release. For example, such a condition might bar the offender from school grounds, parks or playgrounds or the company of under-age children.

National Defence sent nine notices. Seven concerned sharing information with family members following the death of a Canadian Forces member.

The remaining notices came from Transport Canada, Public Works & Government Services Canada, Agriculture & Agri-Food Canada, Health Canada, Indian & Northern Affairs Canada, the Immigration & Refugee Board, the Treasury Board Secretariat, Solicitor General Canada, the Office of the Auditor General of Canada, the Public Service Commission of Canada, the Ombudsman for National Defence/Canadian Forces, the Commission for Public Complaints against the RCMP, CSIS and the National Parole Board.

Inquiries

The Office responds to thousands of inquiries from the general public seeking advice and assistance on a wide variety of privacy-related issues dealing with federal government institutions.

The most common inquiry our Office received during the 2003/2004 year about the *Privacy Act* regarded accessing personal information held by a federal department. These inquiries were made by federal employees and citizens alike. Inquirers were also concerned about how well certain federal departments were protecting their personal information.

Inquiry statistics

(April 1 2003 to March 30, 2004)

Telephone inquiries received	2,580
Written inquiries received (letter, e-mail and fax)	2,148
Total number of inquiries received	4,728

Top ten departments by complaints received

For the year ending March 31, 2004

Organization	Total	Access to Personal Information	Time	Privacy	Other
Correctional Service of Canada	2,760	1,235	1,335	190	
Health Canada	485	2	3	480	
Canada Customs and Revenue Agency	255	103	72	80	
Citizenship and Immigration Canada	132	48	75	9	
Royal Canadian Mounted Police	129	78	34	17	
National Defence	80	32	17	31	
Canada Post Corporation	72	13	24	35	
Human Resources Development Canada	65	21	10	34	
Justice Canada	23	8	10	5	
Foreign Affairs and International Trade	22	4	10	8	
Others	183	91	39	53	
Total	4,206	1,635	1,629	942	0

Complaints received by complaint type

For Complaints Received between 01/04/2003 and 31/03/2004

Complaint Type	Count
Access	1,612
Collection	535
Correction – Notation	20
Correction – Time Limits	27
Extension Notice	28
Inappropriate Fees	1
Language	2
Retention and Disposal	17
Time Limits	1,574
Use and Disclosure	390
Total	4,206

Complaints received by respondent

For Complaints Received from: 01/04/2003 to 31/03/2004

Agriculture & Agri-food Canada	8
Auditor General of Canada, Office of	1
Bank of Canada	1
Business Development Bank of Canada	1
Canada Revenue Agency	265
Canada Post Corporation	72
Canada Firearms Centre	4
Canadian Food Inspection Agency	4
Canadian Heritage	1
Canadian Human Rights Commission	2
Canadian Museum of Civilization	4
Canadian Radio-Television and Telecommunications Commission	3
Canadian Security Intelligence Service	20
Canadian Space Agency	4
Canadian Tourism Commission	4
Citizenship & Immigration Canada	132
Commissioner of Official Languages, Office of the	1
Correction Investigator Canada, The	5
Correctional Service Canada	2,760
EDULINX Canada Corporation	1

Complaints received by respondent (cont.)

For Complaints Received from: 01/04/2003 to 31/03/2004

Environment Canada	1
Finance Canada, Department of	1
Financial Transactions & Reports Analysis Centre of Canada	1
Fisheries & Oceans	5
Foreign Affairs & International Trade Canada	22
Health Canada	485
Human Resources Development Canada	65
Immigration & Refugee Board	15
Indian & Northern Affairs Canada	2
Industry Canada	2
Justice Canada, Department of	23
Military Police Complaints Commission	5
National Archives of Canada	4
National Defence	80
National Gallery of Canada	1
National Parole Board	19
National Research Council Canada	3
Ombudsman National Defence and Canadian Forces	1
Pension Appeals Board Canada	1
Privy Council Office	5
Public Service Commission Canada	4
Public Works and Government Services Canada	5
Royal Canadian Mint	1
Royal Canadian Mounted Police	129
Solicitor General Canada	8
Statistics Canada	4
Status of Women Canada	2
Transport Canada	10
Treasury Board of Canada Secretariat	5
Veterans Affairs Canada	4
Total	3,134

Closed complaints by complaint type

For Complaints Closed between 01/04/2003 and 31/03/2004

Complaint Type	Count
Access	782
Collection	539
Correction – Notation	14
Correction – Time Limits	16
Extension Notice	30
Inappropriate fees	1
Language	2
Retention & Disposal	15
Time Limits	1,511
Use and Disclosure	224
Total	3,134

Closed complaints by origin

For complaints closed between 01/04/2003 and 31/03/2004

Province/Territory	Total
Alberta	658
British Columbia	1,128
International	18
Manitoba	65
National Capital Region (ON)	140
National Capital Region (QC)	22
New Brunswick	41
Newfoundland	8
Nova Scotia	27
Nunavut	1
Ontario	315
Prince Edward Island	1
Quebec	560
Saskatchewan	150
Total	3,134

Complaints by complaint type and finding

For complaints closed between 01/04/2003 and 31/03/2004

	Discon- tinued	Not well- founded	Resolved	Settled in course of investigation	Well- founded	Well- founded & Resolved	Total
Access	40	477	6	177	19	63	782
Collection	6	503	3	14	12	1	539
Correction – Notation	0	10	0	2	0	2	14
Correction – Time Limits	1	1	0	0	14	0	16
Extension Notice	0	16	0	0	14	0	30
Inappropriate fees	1	0	0	0	0	0	1
Language	0	2	0	0	0	0	2
Retention & Disposal	1	5	0	6	1	2	15
Time Limits	294	140	0	11	1,066	0	1,511
Use & Disclosure	23	89	2	55	54	1	224
Total	366	1,243	11	265	1,180	69	3,134

Closed complaints by respondent

For complaints received from 01/04/2003 to 31/03/2004

Federal Institution	Total
Agriculture & Agri-food Canada	6
Bank of Canada	1
Business Development Bank of Canada	1
Canada Customs & Revenue Agency	252
Canada Post Corporation	46
Canadian Firearms Centre	3
Canadian Food Inspection Agency	4
Canadian Heritage	3
Canadian Human Rights Commission	1
Canadian International Development Agency	1
Canadian Museum of Civilization	3
Canadian Radio-Television and Telecommunications Commission	4
Canadian Security Intelligence Service	48
Canadian Space Agency	1

Closed complaints by respondent (cont.)

For complaints received from 01/04/2003 to 31/03/2004

Citizenship & Immigration Canada	92
Commission for Public Complaints Against the RCMP	1
Commissioner of Official Languages, Office of the	1
Communication Canada	1
Correctional Investigator Canada, The	4
Correctional Service Canada	1,636
Environment Canada	6
Finance Canada, Department of	1
Fisheries & Oceans	11
Foreign Affairs and International Trade Canada	16
Health Canada	488
Human Resources Development Canada	51
Immigration & Refugee Board	18
Indian & Northern Affairs Canada	3
Industry Canada	7
Justice Canada, Department of	56
Military Police Complaints Commission	4
Montreal Port Authority	1
Nanaimo Port Authority	1
National Archives of Canada	3
National Defence	109
National Parole Board	23
National Research Council Canada	4
Natural Resources Canada	1
Natural Sciences and Engineering Research Council of Canada	1
Office of the Superintendent of Financial Institutions Canada	2
Ombudsman National Defence & Canadian Forces	1
Privy Council Office	3
Public Service Commission Canada	9
Public Works & Government Services Canada	14
Royal Canadian Mounted Police	164
Solicitor General Canada	11
Statistics Canada	1
Transport Canada	5
Treasury Board Of Canada Secretariat	8
Veterans Affairs Canada	3
Total	3,134

Completed investigations and results by respondent

For Complaints Closed between 01/04/2003 and 31/03/2004

Respondent	Discon- tinued	Not Well- founded	Resolved	Settled in course of investiga- tion	Well- founded	Well- founded & Resolved	Total
Agriculture & Agri-food Canada	1	1	0	2	2	0	6
Bank of Canada	0	0	0	1	0	0	1
Business Development Bank of Canada	0	1	0	0	0	0	1
Canada Customs & Revenue Agency	5	94	2	65	60	26	252
Canada Post Corporation	7	14	1	14	7	3	46
Canadian Firearms Centre	0	1	0	2	0	0	3
Canadian Food Inspection Agency	1	2	0	0	1	0	4
Canadian Heritage	0	2	0	1	0	0	3
Canadian Human Rights Commission	0	0	0	0	1	0	1
Canadian International Development Agency	0	1	0	0	0	0	1
Canadian Museum of Civilization	3	0	0	0	0	0	3
Canadian Radio- Television & Telecommunications Commission	0	2	0	2	0	0	4
Canadian Security Intelligence Service	1	43	0	4	0	0	48
Canadian Space Agency	0	0	0	0	1	0	1
Citizenship & Immigration Canada	12	25	0	13	41	1	92
Commission for Public Complaints Against the RCMP	0	1	0	0	0	0	1
Commissioner of Official Languages, Office of the	0	0	0	0	1	0	1

Completed investigations and results by respondent (cont.)

For Complaints Closed between 01/04/2003 and 31/03/2004

Respondent	Discon- tinued	Not Well- founded	Resolved	Settled in course of investiga- tion	Well- founded	Well- founded & Resolved	Total
Communication Canada	0	1	0	0	0	0	1
Correctional Investigator Canada	0	0	0	0	4	0	4
Correctional Service Canada	308	357	2	46	911	12	1,636
Environment Canada	3	1	0	2	0	0	6
Finance Canada, Department of	0	1	0	0	0	0	1
Fisheries & Oceans	2	5	0	3	0	1	11
Foreign Affairs & International Trade Canada	3	6	1	5	1	0	16
Health Canada	0	481	0	4	2	1	488
Human Resources Development Canada	1	25	1	9	9	6	51
Immigration & Refugee Board	0	3	0	1	10	4	18
Indian & Northern Affairs Canada	0	2	0	1	0	0	3
Industry Canada	0	6	0	0	1	0	7
Justice Canada, Department of	0	7	0	41	7	1	56
Military Police Complaints Commission	0	4	0	0	0	0	4
Montreal Port Authority	0	1	0	0	0	0	1
Nanaimo Port Authority	0	0	1	0	0	0	1
National Archives of Canada	0	0	0	1	2	0	3
National Defence	7	21	0	19	52	10	109
National Parole Board	2	19	0	0	2	0	23
National Research Council Canada	1	2	0	0	1	0	4
Natural Resources Canada	0	1	0	0	0	0	1

Completed investigations and results by respondent (cont.)

For Complaints Closed between 01/04/2003 and 31/03/2004

Respondent	Discon- tinued	Not Well- founded	Resolved	Settled in course of investiga- tion	Well- founded	Well- founded & Resolved	Total
Natural Sciences and Engineering Research Council of Canada	0	1	0	0	0	0	1
Office of the Superintendent of Financial Institutions Canada	0	2	0	0	0	0	2
Ombudsman National Defence and Canadian Forces	1	0	0	0	0	0	1
Privy Council Office	0	2	0	0	1	0	3
Public Service Commission of Canada	0	4	0	1	4	0	9
Public Works and Government Services Canada	2	7	0	1	4	0	14
Royal Canadian Mounted Police	4	79	1	25	52	3	164
Solicitor General Canada	0	10	0	1	0	0	11
Statistics Canada	0	1	0	0	0	0	1
Transport Canada	2	2	0	0	0	1	5
Treasury Board of Canada Secretariat	0	4	2	0	2	0	8
Veterans Affairs Canada	0	1	0	0	2	0	3
Total	366	1,243	11	265	1,180	69	3,134

PRIVACY PRACTICES AND REVIEWS

The Office of the Privacy Commissioner promotes compliance with Canada's two privacy laws through the conduct of privacy audits and compliance reviews. The Office serves as a source of in-house expertise providing assistance and advice to both public and private sector institutions. With the introduction of the Treasury Board Secretariat's *Privacy*

Impact Assessment (PIA) Policy in May 2002, the Office has also assumed responsibility for reviewing and commenting on the PIAs prepared by federal government institutions.

Audits and compliance reviews under the *Privacy Act*

During the past year, the Office conducted Section 37 reviews of the personal information-handling practices of the Canada Industrial Relations Board (CIRB) and the Canadian Forces Grievance Board (CFGGB). We selected these two institutions not because of any suspicion of non-compliance with acceptable privacy practices, but rather because they are small institutions which have in the past escaped the kind of scrutiny given to larger government institutions with significant personal information holdings.

The purpose of the CIRB and CFGGB reviews was to provide guidance and education on privacy matters. This is particularly important in small institutions, where the resources available to devote to privacy are relatively limited. We looked at the practices surrounding the collection, use, disclosure, protection, retention and disposal of personal information, both in hard copy files and electronic format. We also examined the institutions' public listings in Info Source, contracting-out activities, staff awareness of their rights and obligations under the *Privacy Act*, tele-work arrangements, workplace surveillance and the security issues relating to the electronic transmission of information.

The Canada Industrial Relations Board

The CIRB is the independent, quasi-judicial tribunal which interprets and administers Part 1 (Industrial Relations) and certain provisions of Part II (Occupational Health and Safety) of the *Canada Labour Code*. The Board certifies trades unions, investigates unfair labour practices, orders an end to unlawful strikes and lockouts, decides jurisdictional issues, deals with the complexities of corporate mergers and sales and offers mediation and arbitration services for dispute resolution.

The compliance review was conducted at the CIRB's head office in Ottawa and at its regional offices in Toronto and Vancouver. The review found that the Board's personal information handling practices generally comply with the fair information principles established in sections 4 to 8 of the *Privacy Act*. However, our Office identified several matters requiring remedial attention, including the need to develop policies and protocols regarding the protection of operational files and information contained in portable computers carried outside the physical confines of the CIRB. As well, case files required proper identification according to their respective security designations, and attention was needed to properly dispose of records in accordance with established retention and disposition schedules.

The Canadian Forces Grievance Board

Our examination of the Board's operations revealed a high level of compliance with the *Privacy Act* and its fair information principles. However, the review did remark some forms used by the Board to collect personal information required enhancements to ensure that individuals were informed of the purpose of the collection. The review also indicated the need to establish a policy governing the use of faxes to transmit personal information.

At the end of the reviews, the CIRB and the CFGB were issued reports with our findings. We have recently issued our final reports and are awaiting responses from the CIRB and the CFGB to the recommendations contained therein.

Anti-terrorism survey

In addition to these two audits, our Office followed through with an undertaking, discussed in last year's Annual Report, to assess the impact of anti-terrorism measures adopted in the wake of September 11 2001 on the privacy of Canadians. To this end, we conducted reviews of the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment Service (CSE).

The objectives of the reviews were: to determine what had changed in terms of the legislative authorities and operational programs of the RCMP, CSE and CSIS as a result of the anti-terrorism measures introduced by the Government of Canada under its Anti-Terrorism Plan; to examine any new initiative planned or implemented by the organizations subsequent to September 11, 2001, which would impact on the privacy of Canadians; and to assess the extent to which the management of personal information under the new initiatives are in compliance with the fair information practices enunciated in the *Privacy Act*.

Reviews of CSIS and CSE

With regards to CSIS and the CSE, it should be noted that the scope of the reviews did not include commenting on the broader issues of the Government of Canada's national security or foreign intelligence gathering activities. Rather, the focus was to assess the impact of anti-terrorism measures on the personal information handling practices of these institutions. Our inquiries suggest that the events of September 11, 2001, have not resulted in fundamental changes to the management of personal information held under the control of the CSIS and the CSE. Based on our examination of selected documentation and on the responses of CSIS and CSE officials who were interviewed, no substantive *Privacy Act* issues or concerns were identified.

Reviews of the RCMP

The compliance review at the RCMP involved an examination of three primary initiatives: Integrated National Security Enforcement Teams (INSETs); Integrated Border Enforcement Teams (IBETs); and the creation of the Financial Intelligence Branch. While our review revealed a high degree of compliance with the *Privacy Act*, we did have concerns regarding the agreements or arrangements governing the sharing of personal information between the RCMP and its INSET and IBET partners. The matter has been the subject of ongoing discussions with the RCMP.

Cross-border flow of personal information

On the subject of disclosure, a number of programs and activities established by federal Government institutions and agencies provide for the disclosure of personal information about Canadian citizens and residents to departments and agencies of the United States government. During this fiscal year, the Office completed an examination of agreements, arrangements and memoranda of understanding between Canada and the United States that include provisions for the sharing of personal information. Our review found that many of the sharing agreements were deficient in terms of containing adequate privacy protection provisions.

The cross border flow of personal information raises serious privacy risks relating to the jurisdictional differences affecting the protection of personal information, the security of personal information in transit, and the adequacy of legal instruments governing the management of the information shared. Issues related to the trans-border flow of personal information will be a key area of review for the Office during the next fiscal year. To this end, we are conducting an audit of the trans-border information sharing activities of the newly constituted Canadian Border Services Agency (CBSA).

The Canadian Firearms Program

During the course of the year, we continued close monitoring of the Canadian Firearms Program, which was subject to a review by this Office in 2001. Some of the recommendations we made in 2001 have been implemented. The RCMP, for example, adopted our 2001 recommendations to limit Firearms Officer access to the Police Information Retrieval System (PIRS) system and to operational files. We have also followed up on a number of outstanding issues referred to in our 2001 comprehensive Firearms Report, such as outsourcing, international information sharing agreements and the use of supplementary questionnaires.

One of the difficulties in reviewing the Firearms Program is that it has been very much a moving target due to persistent legislative, policy, administrative and information technology (IT) changes to the Program. In the past year, for example, the Auditor General issued her report on the value for money of the program which recommended changes to it; the program was transferred from the Minister of Justice to the Minister of the Solicitor General (now the Department of Public Security and Emergency Preparedness Canada (PSEPC)); a new position of Firearms Commissioner has been created; Bill C-10 was passed by Parliament; and Minister Guarnieri was given the mandate in January 2004 to conduct a full program review.

Some of our observations and findings from the 2001 report, and from our more recent review have been affected by these on-going changes. That said, we have made some significant progress with the Canada Firearms Centre to address the outstanding issues in light of the current state of affairs. We will report on further progress in next year's Annual Report.

Other compliance activities

In addition to compliance audits, our Office also undertakes reviews of submissions from both federal government and private sector organizations and offers advice on a broad range of compliance issues. Some of these compliance review activities are mandated under the *Privacy Act* and the *PIPEDA*, while others are mandated under federal government policy. Other review activities have come about through institutional arrangements involving voluntary consultation with the Office on privacy matters. Human Resources and Skills Development Canada's (HRSDC) - formally the Department of Human Resources Development Canada (HRDC) - *Governance Protocol for the Databank Review Committee* is a case in point.

HRSDC databank review

As described in our earlier reports, HRSDC developed a review procedure to deal with policy analysis, research and evaluation activities involving the linking of separate databanks. Part of this procedure includes consultation with our Office. During the past year, the Office has analyzed and commented on 20 HRSDC submissions, including an evaluation of the Employment Insurance program since the 1996 reforms, the success of various Labour Market Development Agreements and studies relating to the Canada Student Loans Program. Over the course of the last several years we have witnessed a marked improvement in the completeness and quality of the submissions we have received. This is evidence of the seriousness with which HRSDC regards its data linkage activities, and its dedication to ensuring that such linkages are undertaken in accordance with privacy best practice principles.

Policy on Data Matching

Under the Treasury Board Secretariat of Canada's *Policy on Data Matching*, federal government departments and agencies are required to notify the Office of any data matching proposal. The purpose of this notification is to afford the Office an opportunity to review and comment on the proposal so as to ensure that the data matching complies with the requirements of the *Policy*. Over the course of the last fiscal year, our Office received 10 data matching submissions. These submissions complied with the nominal requirements of the *Policy*, though we have found it necessary to remind departments of their duty to inform the public when their personal information is to be matched against other government information holdings. In most cases such notification will not prejudice the use of the information.

Disclosure of personal information to a third party

Pursuant to paragraphs 7(2)(c) and 7(3)(f) of the *PIPEDA*, private sector organizations are required to notify our Office when personal information is to be disclosed to a third party without the consent of the individual for "statistical, scholarly study or research purposes."

Our role is to provide advisory services to a number of federal government departments and to serve as a resource for private sector organizations seeking information on the application of privacy best practice principles to their respective commercial activities.

Organizations must demonstrate in their submissions that; 1) the information contemplated for disclosure will be used solely for "statistical, scholarly study or research purpose; 2) the purpose of the disclosure cannot be achieved without the information being in an identifiable format; 3) obtaining consent from the individuals involved would be "impracticable"; and 4) the disclosing organization has taken such measures as are appropriate to ensure that the information will be used in a manner that preserves its confidentiality.

In the course of the last fiscal year the Office has received 4 notifications under paragraph 7(3)(f) of the *PIPEDA*. Most of these submissions involved the use and disclosure of medical information for health research purposes. These submissions have been of varying levels of completeness and quality. While relying on a very small sample, it is evident that organizations are unsure of their obligations under paragraph 7(3)(f) of the *PIPEDA*. Particularly problematic is the question of when and under what circumstances obtaining consent would be "impracticable." Over the course of the next fiscal year, the Office will commit resources to develop a guide to assist organizations in understanding their obligations under section 7 of the law, and in preparing their submissions to the Office of the Privacy Commissioner.

Other consultation and advisory services

The Office also provides less formal advice, comments, and recommendations to numerous federal departments as needed. Departments aided in this way include the Treasury Board of Canada, Statistics Canada, Health Canada, Human Resources and Skills Development Canada, Indian and Northern Affairs Canada, the Canada Revenue Agency and the Canadian Border Services Agency.

Consultations were undertaken on a wide variety of issues, including

- A Privacy Impact Assessment Audit Guide
- Data matching policies
- Policies for use of the Social Insurance Number (SIN)
- Privacy best practices for departments
- Legislative and policy reform
- Privacy risks of specific programs and initiatives

The Office also assists private sector organizations in assessing privacy risks, instilling best practices and developing appropriate privacy policies.

Privacy Impact Assessments

The Treasury Board Secretariat of Canada's *Policy on Privacy Impact Assessments* (PIA) has now been in effect since May 2002. When first launched, the *Policy* was enthusiastically welcomed by members of the professional privacy community, and with good reason. For the first time federal Government departments and agencies were equipped with a tool that could be used to forecast the impacts on privacy relating to a given initiative, to assess and weigh the impacts in a consistent fashion, and to come up with strategies to mitigate those impacts or risks. By requiring privacy principles to be considered in the planning, design, and implementation phases of a project, the *Policy* helps to give effect to those principles in a way that is tangible and demonstrable.

The *Policy* was the first of its kind to make PIAs mandatory for all new federal government programs or services that raise potential privacy issues. The *Policy* requires that federal government departments and agencies notify the Privacy Commissioner when undertaking a PIA, giving the OPC an opportunity to review and comment on the project. This provides added assurance that risks relating to a given initiative have been properly identified and that mitigating measures proposed to deal with those risks are reasonable and appropriate.

OPC perspective on PIAs

Since the *Policy* came in effect in May 2002, the OPC has received over 100 PIAs and Preliminary Privacy Impact Assessments (PPIA) reports for examination. As could be expected with the launch of any new policy directive, many of the PIA and PPIA submissions we received for review in the first year ranged in completeness and quality. Common errors and omissions we observed with those early submissions were itemized in the Commissioner's Annual Report for fiscal year 2002-2003.

In the course of the last fiscal year, however, we have observed a marked improvement in the completeness and quality of the PIA and PPIAs we have received. We see this improvement as evidence that departments are learning from consultations with our Office. This improvement can also be attributed to the efforts of the Treasury Board Secretariat to educate departments on the requirements and methodologies of the *Policy*. Treasury Board's "PIA e-learning tool" which became available on-line in the fall of 2003, has been a valuable resource. We would encourage anyone interested in learning more about the PIA process to visit Treasury Board's web site at: www.tbs-sct.gc.ca.

Looking ahead

While we have been impressed by the general improvement in the quality of the PIA and PPIA submissions we receive, there is one frequent omission that continues to give us cause for concern. Many PIAs fail to include an action plan to actually address and resolve the privacy risks they identify. Our Office will be working with departments and agencies to encourage the inclusion of such action plans in all PIAs, and to help departments identify the appropriate next steps.

However, there are strong indications that the *Policy* is achieving its primary purpose; that of increasing awareness among government personnel at all levels of the importance of privacy in day-to-day administrative functions. Departments can no longer create new databases, link information holdings, enter into information sharing arrangements with other departments, or launch new programs or services, without considering their potential impact on privacy.

Just as departments have struggled with limited resources to comply with the *Policy*'s requirements, so too has the OPC challenged to allocate sufficient resources to effectively perform its advisory role under the *Policy* without supplementary resources.

The reduction of staff available within the OPC to review PIAs and PPIAs, combined with an increase in the volume of submissions over the last fiscal year has led to delays in providing departments with feedback. The OPC is endeavouring to address this resource deficit and we are optimistic that a remedy will be found.

The reduction of staff available within the OPC to review PIAs and PPIAs, combined with an increase in the volume of submissions over the last fiscal year has led to delays in providing departments with feedback. The OPC is endeavouring to address this resource deficit and we are optimistic that a remedy will be found.

We believe no other government initiative since the enactment of the *Privacy Act* itself has made as significant a contribution to fostering a privacy-sensitive culture within the federal public service.

However, our Office has found it a challenge to perform its advisory role under the PIA Policy without the allocation of supplementary resources. A lack of human and monetary resources for this purpose for this purpose and a great increase in the volume of submissions over the fiscal year has led to unfortunate delays in providing departments with the feedback they need. OPC will continue to press for a resolution to this resource deficit so that we may avoid further delays, clear the current backlog, and adequately support departments in applying the TBS PIA Policy.

IN THE COURTS

Section 41 of the *Privacy Act* allows an individual, following the results of an investigation of a complaint by the Privacy Commissioner, to apply to the Federal Court for review of the decision of a Government institution to refuse the individual access to personal information. From the time the *Privacy Act* came into force in 1983 to March 31, 2004, approximately 141 applications for review have been filed in the Federal Court. Eleven of these were filed in the year ending March 31, 2004.

Section 42 of the *Privacy Act* allows the Commissioner to appear in Federal Court. The Commissioner can apply to the Federal Court for review of the decision of a Government institution to refuse access to personal information, with the consent of the individual who requested the information. The Commissioner can appear before the Court on behalf of an individual who has applied for review under section 41. Or, with leave of the Court, the Commissioner can appear as a party to any review applied for under section 41.

The Commissioner has also intervened on numerous occasions in other litigation arising outside of the *Privacy Act* in which issues involving interpretation of the *Act* were raised.

In last year's annual report we reported on the conclusion of a number of cases in which the Commissioner had been actively involved. In the past fiscal year there has been no significant litigation concerning interpretation of the *Privacy Act* that required the intervention of the Commissioner.

PART TWO

Report on the *Personal Information Protection and Electronic Documents Act*

INTRODUCTION

The Personal Information Protection and Electronic Documents Act (PIPEDA) sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

Since the *Act* took effect on January 1, 2001, it has applied mainly to the commercial activities of what are known as federal works, undertakings or businesses, such as transportation and telecommunications companies, banks and broadcasters. It also applies to the personal information of employees in those companies, and it applied to personal information that is sold, leased, or bartered across provincial or national boundaries by provincially regulated organizations.

As of January 1, 2002, the personal health information collected, used or disclosed by these organizations is also covered.

On January 1, 2004, *PIPEDA* extended to cover the collection, use or disclosure of personal information in the course of all commercial activities in Canada, except in intraprovincial collection, use and disclosure where there is substantially similar legislation.

PIPEDA now also covers all cross border collection, uses and disclosures and federal works, undertakings and businesses.

INVESTIGATIONS AND INQUIRIES

This Office received 302 complaints under *PIPEDA* between January 1 and December 31, 2003, which is approximately the same number as in 2002. As in previous years, complaints were filed against a variety of organizations and dealt with allegations that individuals' privacy rights had been violated. Once again, the largest number of cases, 42%, were filed against organizations in the banking sector; the telecommunications and

broadcasting sector accounted for 26% of cases. The percentage of complaints against transportation companies rose slightly to 19%. Credit reporting agencies accounted for a further 4% of the total, and the remaining 9% involved rewards programs, internet service providers and aboriginal band councils.

The number of cases finalized in 2003 rose to 278, a 58% increase from the previous year. Complaints were concluded as follows:

Not well-founded	115	(41%)
Well-founded	97	(35%)
Resolved	14	(5%)
Settled	4	(2%)
No jurisdiction	5	(2%)
Discontinued	43	(15%)

Definitions of findings under *PIPEDA*

Not well-founded: This finding means that the investigation uncovered no or insufficient evidence to conclude that an organization violated the complainant's rights under *PIPEDA*.

Well-founded: This finding means that an organization failed to respect a provision of *PIPEDA*.

Resolved: This finding means that the allegations are substantiated by the investigation; however, the organization has taken or has committed to take corrective action to remedy the situation, to the satisfaction of this Office.

Settled during the course of investigation: This disposition is used when the Office has helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.

Discontinued: This means that the investigation was terminated before all the allegations were fully investigated. A case may be discontinued for any number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

No jurisdiction: This means that it has been determined during investigation that *PIPEDA* does not apply to the organization or to the activity that is the subject of the complaint.

Early resolution: This is a new type of disposition, which the Office will begin using in 2004. It will be applied to situations where the issue is dealt with before a formal investigation is undertaken. For example, if an individual files a complaint about an issue that the Office has already investigated and found to be compliant under *PIPEDA*, we would explain this to the individual. This disposition would also be used when an organization, upon learning of the allegations, addresses the issue immediately and to the satisfaction of the complainant and this Office.

Select cases under *PIPEDA*

SAFEGUARDING OF PERSONAL INFORMATION

Wedding bell blues

Overview

She was only trying to be helpful. That is what the bank employee in this case undoubtedly believed when she gave the fiancée of a customer a copy of his student loan application, containing information about his loans and credit card, from the previous year. She thought it could assist him in filling out another form for the new school term. She also probably thought it was not a big deal to leave his banking file out on her desk, where the fiancée could see it, while she went to search for a document.

It was, in the end, a very big deal. The young woman knew that her boyfriend had a student loan, but she did not know the full amount of his debt – until she saw it in the file. As a result, she called the wedding off.

The employee acknowledged her error. She thought the fiancée was acting as the boyfriend's agent because the woman, who had attended the bank to drop off some documents for him, referred to herself as his "go-between." The employee stated that in the future, she would ensure that she had a signed document indicating that someone was acting on another's behalf before discussing any personal information.

Actions taken by the OPC

We noted that despite the “go-between” comment, the bank employee did not have the student’s authorization in writing, contrary to the bank’s own policy. Without documentary evidence that the student authorized the disclosure, we found that the bank had contravened the requirement for consent under the *Act*, and concluded that the complaint was well-founded.

Although it was a one-time incident, it was an example of the serious ramifications that privacy disclosures – however inadvertent or well-intentioned – can have.

More than just fruits and vegetables

Overview

An individual had hoped to conduct some business at her bank’s kiosk located in a nearby supermarket. While she waited for service, she noticed a computer terminal in an open area. The monitor was live, and assuming that it was for the public to use to obtain general banking information, she typed in her name and address as prompted. The computer displayed information related to her accounts with the bank, including credit card numbers, limits, and balances. She had not been asked for any password or user identification.

Later, when she was sitting with a bank employee, she was able to see him entering his password, which she claimed appeared on screen in clear text, when he logged onto another computer. (She stated that the screen was positioned such that she could see it.) Concerned about the bank’s apparent lack of safeguards, she brought her concerns to our attention.

The kiosk branch in question comprised an ABM for public use, an enclosed business office with a computer terminal for employee use only, and one other computer terminal situated in an open area. This terminal was also intended for employee use, but there was no sign posted to that effect. On the day in question, two employees were working. One was away at the time of the incident, and the other was busy with a customer in the enclosed office.

According to the bank, this incident was a simple case of employee error. The last employee to use the open-area computer had forgotten to log off – an infraction of the bank’s own security policy and procedures.

The bank took two remedial measures as a result of the complaint. First, it sent advisories to employees of in-store offices, placed a message on its intranet site, and included some formal guidelines in training manuals for new employees. Second, it installed a new computer system with a password-protected screensaver that activates automatically if the keyboard remains untouched for 15 minutes.

As for the allegation that she could discern the password used by the bank employee, the bank said that, with the computer system in use at the time, passwords appeared on screen in the form of symbols, not in recognizable clear-text characters. The bank suggested that the complainant had either mistaken the employee's user ID or other log on information for his password. It also suggested that she perhaps had recognized the password by looking at the keyboard while the employee was typing rather than from the computer screen.

The complainant countered that it did not matter how she had recognized the characters. Bank employees logging on to computers should not allow customers to see either the computer screen or the keyboard.

Actions taken by the OPC

We considered this complaint well-founded. We noted that the bank had created a considerable risk of unauthorized access to customers' personal information when it installed in open areas of its kiosk branches computers that were often left unattended. In considering whether the bank had instituted appropriate safeguards to mitigate this risk and protect the information, we determined that:

- The bank's primary safeguard at the time of the incident was an instruction in a security manual to the effect that employees should log off when about to leave a computer unattended.
- A bank employee's failure to follow this instruction resulted in the complainant gaining unauthorized access to sensitive personal information.
- Although no improper disclosure to a third party occurred, the same neglect by the employee had created a significant potential for such a disclosure.

In the circumstances, the safeguard upon which the bank relied was ineffective and inappropriate. We therefore found the bank in contravention of the requirement under *PIPEDA* for appropriate safeguards.

As for the remedial measures taken by the bank, we felt that, although the automatic shutoff was an improvement, this measure would not prevent access during the 15-minute time delay and therefore could not be considered an adequate safeguard. A safeguard was needed that would protect sensitive personal information at all times.

As for the second remedial measure, we noted that even though the employee in this incident knew the rule he had neglected to follow it. Taking the human factor into account, we were not convinced that a reinforced instruction was likely to provide any more effective protection than the original form of instruction. Indeed, we were concerned that relying on the new 15-minute cut-off would actually make employees complacent and less likely to follow the rule of logging off manually.

In spite of the remedial measures, we felt there continued to be an unacceptable potential for unauthorized access to customer information via the computers placed in areas open to the public.

We recommended that the bank:

- Review its information security policy and procedures specific to the operation of its kiosk branches and take appropriate measures to ensure that access to any computers whereby customers' personal information may be obtained is restricted to authorized bank employees; and
- Take appropriate measures to ensure that customers are prevented from seeing passwords and other identifiers used by employees to log on to computers.

The Office is currently following-up with the organization to ensure that recommendations have been implemented.

Lost and found

Overview

An employee of a company complained to us when a co-worker found a letter concerning the complainant in a reference binder. The binder in question was reserved for employee use and was accessible to anyone on the work site. The letter summarized a meeting the complainant had, some six years earlier, with his superiors regarding problems he was having at work. In the letter was a recommendation for a new posting, as well as certain measures to help him with a number of personal problems he was having at the time.

Two letters, relating to two other employees, were also found at the same location. These documents concerned personal problems that these individuals had been having at work.

The company could not explain how these letters ended up in a reference binder, suggesting that the binders had been misplaced or moved and then reopened several years later. We noted that the way the company handled documents containing the personal information of employees had completely changed over the last several years.

Actions taken by the OPC

In our view, such highly sensitive personal information, referring to an employee's personal problems, required special protection. Although our investigation could not determine how these letters ended up in the binder, we concluded that there had been gaps in the company's safeguards to protect the personal information of employees. We also noted that such documents had been kept far longer than necessary to fulfil the company's stated purposes.

While we concluded that the complaint was well-founded, we were pleased that the company sent the complainant a letter of apology during the investigation.

IDENTIFYING THE PURPOSE OF THE COLLECTION OF PERSONAL INFORMATION

The baggage we carry

Overview

All she wanted was to find her missing baggage. She certainly did not expect that to do so, she would have to provide the airline that misplaced it with her SIN, her date of birth, and her occupation on the baggage claim form.

Though not happy about giving this information, the complainant in this case did eventually complete and submit a baggage declaration form so that the airline would pursue the matter. None of the items of personal information requested on the form were designated as optional. The form did identify two purposes for collecting the information – tracing baggage and serving as the basis of a claim.

Actions taken by the OPC

What the form did not identify, but our investigation revealed, was that the information collected would be filed in a tracing system used by air transport organizations worldwide and therefore accessible to other parties. In addition, the form did not specify that serving “as the basis for a claim” actually meant not only processing a claim, but also investigating the credibility of the claimant.

Our Office learned that the tracing system included an investigation component whereby the airline, following an unsuccessful trace, could crosscheck for prior claims and any suspicious informational inconsistencies possibly indicating fraudulent intent on a claimant’s part. The airline acknowledged that most of the personal information it collected from its form was used as much for the purpose of claims verification as for the purpose of tracing baggage. The airline maintained that not all the information on its form was mandatory. Claimants had discretion to decline to provide an item if they did not feel comfortable in doing so. However, the form itself did not indicate that any of the information it requested was optional, nor did it appear that the airline made a practice of informing claimants that they had any discretion in the matter.

In discussions with the airline, our Office took the following position:

- it is not appropriate for an organization to require the provision of a SIN as an identifier;
- an individual’s occupation is not an appropriate item to request as a means of verifying a claim nor is “company name”;
- date of birth and several of the other items of personal information requested on the claims form should be designated as optional; and
- the form should be revised so as to specify that collected personal information is recorded in a tracing system available to other users, and clarify that claims verification is one of the purposes.

While the airline agreed to revise its form as proposed, to remove SIN from it, and to designate date of birth, passport number, and passport name as optional, it was reluctant to make further concessions.

In our findings, we determined that the airline had not stated its purposes for collecting personal information in such a way that the customer could reasonably understand how

the information was to be used or disclosed. In our view, the airline should have clarified that tracing baggage would involve putting personal information into a tracing system and creating a potential for disclosure to other users of that system. We also stated that the airline should have clarified that serving as the basis of a claim meant verifying the claim as well as processing it. The vaguely stated purposes did not, therefore, constitute a reasonable effort on the company's part to inform individuals of the purposes for which their personal information was to be used or disclosed.

As for the counter agent who had initially collected the complainant's personal information, we determined that she had made no effort to explain to the complainant what was to be done with the information. Although the agent might well have assumed that the complainant would understand that it would be used to trace her baggage, we believed that the agent should have at least informed the complainant of the means by which the information was to be recorded and by which the tracing would be done – that is, the worldwide tracing system.

Noting that knowledge is required as a basis for consent, we stated that the airline should have first informed the complainant of the specific reasons for collecting her personal information. As the company had not done so, it had no valid basis for consent.

Finally, with respect to the fact that the company had required the complainant to complete the entire form as a condition for pursuing the missing baggage, we noted that the purposes for which the information was collected had not been properly specified, as required under *PIPEDA*. We also determined that the airline's collection of SIN, birth date, occupation and company name was excessive and we were satisfied that a reasonable person would not have considered it appropriate to collect such information in the circumstances.

We therefore concluded that this was a well-founded complaint and recommended that the airline:

- follow through with the undertakings previously agreed to;
- designate “business address,” “business telephone,” “e-mail,” and “frequent flyer ID” as optional;
- remove “occupation” and “company name” from the form;
- group all optional items on the form under one heading so that passengers may choose to complete some, all or none of the items;

- specify, at the items “prior address” and “prior telephone number,” that these requests are made solely for the purpose of verifying the claim; and
- instruct its baggage claims agents to explain to the individual the use to be made of personal information collected at the time missing baggage is first reported; to specify that the information is to be filed in the tracing system and made available to other users of the system; and to limit initial information requests to those items that are justifiable in terms of the strict purpose for the initial collection – that is, tracing baggage reported as missing.

The Office is currently following-up with the organization to ensure that recommendations have been implemented.

UNAUTHORIZED USE OF PERSONAL INFORMATION

The cart before the horse

Overview

This Office learned that one branch bank manager had instructed her employees to conduct credit checks on customers, without their knowledge and consent, to determine who might be eligible for overdraft protection. Customers were then later informed that they had been pre-approved for the service. If they accepted, they were asked to sign an authorization for a credit check that had already been performed.

By the time we became aware of it, the bank had already initiated corrective action. During a regular “spot check” conducted by the bank to ensure compliance with bank policies, a deviation in policy at this particular branch was noted. The policy in question stated that employees must obtain a customer’s consent to a credit check when offering him or her overdraft protection. The branch manager was notified, and she corrected the situation immediately.

The bank stated that the manager had misread the consent language for accounts. She mistakenly believed that she could use the consent language referring to a credit update to justify pre-screening for the overdraft protection.

Outcome

As there was no dispute that the branch manager had authorized the collection and use of customers’ personal information without their knowledge and consent, we found

the bank in contravention of the consent requirement under *PIPEDA*. However, as the bank had a proper policy in place, and discovered and corrected the deviation in policy even before the Office became interested in the matter, we concluded that the complaint was resolved.

OBTAINING CONSENT

The ex-wife, her lawyer, the daughter and the collection agent

Overview

One individual complained that a bank, through a collection agency working on its behalf, had been telling his family members and his ex-wife's lawyer about his financial woes. Our investigation established that the collection agent handling the file had indeed contacted the complainant's daughter, his former wife, and her lawyer. In fact, there were a number of telephone conversations between the agent and these individuals. Some calls were placed by the agent; others, by the individuals to the agent. All calls coming into and going out of the agency, as well as summary notes of the calls, were logged into the agency's electronic tracking system. The information in this system could only be altered within two hours after it was originally logged.

Actions taken by the OPC

We could find no evidence that the agent had disclosed specific information regarding the complainant's financial situation, or made any threats about seizing his property, as he alleged.

The bank audits the agency to ensure that its privacy practices are in keeping with those of the bank. The agent, a long-time employee of the company, had signed a number of confidentiality and ethics statements with the agency.

In our findings, we noted that, although *PIPEDA* allows an organization to disclose personal information without knowledge and consent to collect a debt owed by the individual to the organization, it does not confer a *carte blanche* upon an organization to disclose however much information it wishes in pursuit of a debt.

In this case, we established that the only information provided to the ex-wife was a reference to an outstanding debt. Her lawyer declined to provide written confirmation of what the agent disclosed to her. The daughter and the agent contradicted each other's testimony, and we could find no documentary evidence showing that there had been any

excessive disclosure of the complainant's personal information. Given this, we concluded that the complaint was not well-founded since the agent's actions were consistent with the exception to consent in the pursuit of a debt.

Measuring up

Overview

Two employees of a company protested when their employer decided to use statistical data about their work to measure job performance. The information in question – volume, duration, and type of call received by telephone operators – had long been collected to measure and manage workload at the office level. However, when the company began using this information to manage individual performance, the complainants, who were telephone operators, argued that the company was collecting and using statistical data about them without their consent.

We learned that the company had informed its employees of this policy change via group presentations, e-mail, and team and one-on-one meetings. The collection and use of statistics were also discussed in the company's privacy brochure for employees.

The employees received a monthly report containing their individual statistics as compared with predetermined targets or expectations. They also could receive a report containing statistics per shift.

Actions taken by the OPC

We found that the company's purpose, namely to monitor and evaluate the job performance of its employees, was appropriate, and that the company had adequately informed employees of this purpose. As for whether an employer required an employee's express consent to collect and use such information for performance-management purposes, we determined that when an individual agrees to work for a company, he or she is giving implied consent to the conditions of employment. Performance evaluation is one such condition, and one to which the complainants had given their implicit consent when they began working with the company. We concluded that the complaint was not well-founded.

Credit report check-up

Overview

When a couple checked their credit report, they noticed that the credit agency had disclosed their credit information to a particular credit grantor. They had never had any direct dealings with this credit grantor, and were suspicious that the grantor had accessed

their credit file on behalf of its parent company. The parent company was also the wife's former employer, and the adversary in a dispute.

The couple complained to the credit agency, and was told that their concerns would be investigated and the results made known to them. However, when they called three weeks later for an update, a different representative told them that no internal investigation had been initiated.

This same representative told them that they should look into the matter themselves since the parent company in question was not a client of the agency, and the agency therefore had no jurisdiction to investigate. Yet a third representative subsequently promised that the agency would investigate. Skeptical of this promise, the couple complained to us.

Actions taken by the OPC

Our investigation confirmed that the third representative had initiated an investigation. The owner of the parent company admitted to the agency that he had obtained the couple's credit information without their consent through his company's subsidiary. He knew he had broken the rules. But he stated that the circumstances relating to his company's dispute with the wife over possible wrongdoing on her part had compelled him to take such action.

The credit grantor's standard contractual agreement with the agency stipulated that it could only order consumer credit reports for permissible purposes and that it must first obtain all consumer consents required under the applicable provincial credit reporting legislation. The agreement also stated that the agency could immediately terminate or suspend service if it reasonably believed that its client had breached any condition.

The agency did not terminate or suspend service to the offending credit grantor, but rather placed it on a year's probation. The agency assured the Office that this punitive measure would include audits and monitoring of the client's credit information applications. It also promised that further failure to comply would result in termination of the contract.

After completing its investigation, the agency did not inform the complainants of the results for some eight weeks. The agency notified the complainants that the unauthorized credit inquiries had been removed from their files because the client had been unable to prove a legitimate purpose or valid consent. The agency apologized to the complainants for any inconvenience caused.

On the matter of consent, we determined that the credit agency disclosed the couple's personal information without their consent. The issue we had to consider was whether the agency could reasonably be held responsible in the circumstances.

It was clear to us that the agency had not known that the complainants' knowledge and consent were lacking. It was also clear that the agency had presumed, on the basis of a contractual agreement, that the company's purpose was permissible and that consent had been obtained. Therefore, in our opinion, the agency's disclosure had been made in good faith and on reasonable presumption of consent, given the obligations set out in the contract, and thus did not in itself offend the *Act*.

However, when it came to the agency's investigation and the follow-up to its investigation, we were more critical. Under the *Act*, an organization must investigate all complaints it receives and take *appropriate* measures if the investigation shows the complaint to be justified. The agency had found the complaint to be justified and had eventually taken certain measures against its client, but the measures taken – notably, that of putting the client “on probation” – fell short of being appropriate for the following reasons:

- In the first place, the evidence strongly suggested that the measures against the credit grantor had been taken only at the Office's prompting.
- Secondly, it was reasonable that one immediate measure an organization should take at the end of its investigation was to inform the complainant of the results. It appeared, however, that the agency only notified the couple of the results after this Office suggested that it was the appropriate thing to do.
- Thirdly, and most importantly, the measures taken by the agency had not been appropriate in relation to the seriousness of the offence. The agency's agreement warned of “suspension” or “termination” of services for clients reasonably believed to be in breach, but the agency had imposed “probation.” We did not believe that this sanction conveyed a strong enough message to the company that its actions were unacceptable. We noted that punitive measures regarding such privacy breaches should reflect due regard for the integrity of personal information in its care — and ideally should serve as a deterrent to further similar breaches.

We made the following recommendations:

- The agency should consider imposing and enforcing tougher penalties for client organizations in breach of contract relating to access to consumers' personal information. Penalties could begin with suspension of services, followed by a probationary period involving frequent and rigorous audits.
- The agency should develop and strictly apply a policy stipulating the timing and method of informing a complainant of the results of an internal complaint investigation.

The Office is currently following-up with the organization to ensure that recommendations have been implemented

USE OF SOCIAL INSURANCE NUMBERS

To SIN or not to SIN

Overview

A customer objected to a bank using social insurance numbers (SINs) to confirm the identity of credit card applicants with the credit bureaus. The complainant believed that the bank was doing this without properly informing applicants, and obtaining their consent. She also felt that the language of the credit card contract did not clearly indicate that customers had the option of not providing their SINs. Instead, she said the language left the impression that if you did not provide your SIN, you would not get the card.

The bank maintained that its purpose for using the SIN, which was to accurately match the credit history file of creditors was a legitimate one. The bank told us that providing the SIN for this purpose was optional. A customer could refuse to provide it, or ask the bank to remove it from its records.

Both the electronic and the hard copy versions of the application form included a statement about the SIN being used for identification purposes. But neither form mentioned that its provision was optional. In fact, both forms stated that all information must be provided, and that signing the form or clicking the appropriate box indicated agreement to all terms by the applicant.

Actions taken by the OPC

Since the bank had not made a reasonable effort to ensure that the customer was properly informed that providing a SIN was optional, we found that the bank was not obtaining valid, meaningful consent from applicants.

The bank acknowledged that the language on its forms was a problem, and agreed to make changes indicating that the provision of the SIN for credit history file matching purposes was optional. While we were pleased with the bank's undertaking, we stressed that the SIN is not a piece of identification and should not be used as such.

Use of SIN in the private sector

This complaint was representative of the many complaints our Office received in 2003 regarding the use of the SIN for identification purposes by private-sector organizations.

The legislated uses of the SIN have expanded since its creation in 1964 as a client account number in the administration of the Canada Pension Plan and various employment insurance programs. The federal government, in an effort to prevent the SIN from becoming a universal identifier, issued a policy limiting the collection and use of the SIN to specific acts, regulations and programs.

The following summarizes the extent to which the collection of SINs is permissible in the private sector:

- Employers are authorized to collect SINs from employees in order to provide them with records of employment and T-4 slips for income tax and Canada Pension Plan purposes.
- Organizations such as banks, credit unions, brokers and trust companies are required under the *Income Tax Act* to ask for customers' SINs for tax reporting purposes (e.g., interest earning accounts, RRSPs, etc.).
- No private-sector organization is legally authorized to request a customer's SIN for purposes other than income reporting. In the case of a financial institution, there is no legal requirement for the organization to collect the individual's SIN, and no obligation for the individual to supply it, if a customer's account is not of a type that earns interest (e.g., if it is a credit account as opposed to a savings account).

- There is no law prohibiting an organization from *asking* for a customer's SIN, or a customer from supplying the SIN, for purposes other than income reporting.

While there is no legislation that prevents organizations from asking for the SIN for other purposes, such as identification, organizations that are subject to *PIPEDA* must clearly indicate to the customer that provision of the SIN is optional and not a condition of service.

USE OF WEB MONITORING TOOLS

The way the “cookie” crumbled

Overview

An individual was unhappy with one organization's Web site. He told us that he was unable to access the site because he had configured his browser to disable “cookies.” He also claimed that the company's Web site was collecting the personal information of visitors without their knowledge and consent because it did not inform visitors that it placed a cookie on their computers' hard drives.

The organization used both permanent and temporary cookies on its Web site. Cookies collect and store a variety of information. Permanent cookies are stored indefinitely on a user's hard drive unless manually deleted, while temporary cookies are automatically deleted from the user's browser upon logging off a site. Web browsers typically allow users to disable permanent or temporary cookies. The complainant, who had disabled permanent cookies, was unable to proceed through the site in question because it was coded in such a way that it would not let him in until a cookie had been stored on his computer. The company acknowledged that this was caused by an “application glitch” and took steps to ensure that visitors who had programmed their computers to refuse permanent cookies could still use the site.

The organization also admitted that it did not indicate on its Web site or in its company privacy policy that it used cookies. The company, however, told our Office that it was in the process of creating and publishing a comprehensive policy on its use of cookies.

Actions taken by the OPC

In this well-founded complaint, we determined that the information stored by the temporary and permanent cookies was personal information for the purposes of *PIPEDA*.

Although the company did not intentionally deny access to individuals who had disabled permanent cookies and had taken steps to fix the problem, the company had nonetheless denied the complainant access. We also noted that the company had not met the requirement for knowledge and consent under *PIPEDA* regarding its use of cookies. Our Office was pleased, however, that the company agreed to publish a comprehensive policy on its Web site regarding cookies.

EMPLOYEE MEDICAL INFORMATION

The *Personal Information Protection and Electronic Documents Act* applies to the personal, including medical, information of employees in federal works, undertakings, or businesses. In 2003, the Commissioner received a number of complaints from employees alleging that their employers were collecting too much medical information or inappropriately disclosing it. The following are summaries of some notable cases. Also included at the end is an overview of our Office's position to date.

Diagnosis: Too much information

Overview

Several employees of a company complained when their employer required them to provide medical diagnoses for sick leave. These individuals had exceeded the number of days allowed every year for uncertified sick leave, or had what their employer considered a suspicious leave pattern.

The complainants had no problem with their employer asking whether or not they were under a doctor's care, what if any restrictions they might have, and whether they were taking any medications that might affect their ability to work safely. What they did not like was their employer forcing them to provide a *diagnosis* of their illness to justify their sick leave.

The company countered that it needed the diagnosis information for two purposes. One reason involved "at risk" employees. These individuals work in safety-sensitive positions, often in isolation, with long shifts, and physically demanding duties. The company maintained that an employee's physician may not be aware of the employee's job requirements. It believed the company's health and safety officer would be in a better position to judge if it was safe for the employee to return to duty. However, the company could not provide any evidence that it routinely used diagnostic information for such a purpose. Indeed, in one case, it allowed an "at-risk" employee to return to duty even though his doctor had not provided the company with a diagnosis.

The other reason for requiring a medical diagnosis concerned “suspicious absences.” An absence was considered suspect if taken immediately prior to or following vacation leave or during a period when the company had previously refused time off. If the company found the absence questionable, it reserved the right to demand a medical certificate with a diagnosis from the employee.

Following discussions with the Office, the employer decided it would no longer require employees to submit a diagnosis for suspicious absences and to re-examine the requirement for diagnoses in respect of “at risk” employees.

Actions taken by the OPC

In our determinations, we commented that while it was appropriate and reasonable for the employer to require medical certificates when the employees’ absences exceeded the allowable limit for uncertified sick leave, a medical certificate without a diagnosis should have been sufficient. As the employer ultimately acknowledged, it was not necessary to require employees to provide diagnostic information in cases of suspicious absences.

In our opinion, the company did not satisfactorily demonstrate the need to inquire into the nature of the illness to ensure the complainants’ fitness to resume regular duties or to otherwise accommodate their return to the workplace.

Indeed, in the circumstances of these complaints, namely, where the employees had exceeded their allotted annual uncertified sick leave or their absence was suspect, we found it unnecessary and inappropriate for the company to have demanded this information. We therefore concluded that the complaints were well-founded.

We recommended that the company drop its requirement for mandatory inclusion of diagnoses in the medical certifications of employees designated “at risk” and limit its collection of employees’ diagnostic information to cases of clear necessity in the fulfillment of legitimate purposes. We also recommended that the company amend its sick leave policy accordingly.

Finally, we recommended that the organization review its decision to deny medical leave to individuals who refused to provide a medical diagnosis when they had exceeded their allotted annual uncertified sick leave.

The Office is currently following-up with the organization to ensure that recommendations have been implemented.

Diagnosis: Purposes reasonable

Overview

The need for diagnostic information, and to whom medical information is disclosed, were the subjects of complaints made by an individual against her former employer.

At the start of an extended sick leave, the complainant submitted a completed medical form to her employer containing a specific diagnosis from her doctor. Although she provided this information, she objected to the requirement for the diagnosis. She believed that her employer should be content with a general description, such as “illness,” “injury,” or “work-related.”

To her surprise, a few months after submitting the form, the complainant received a letter from the provincial Workers’ Compensation Board, rejecting her claim for compensation for lack of evidence. The Board determined that her disablement was not work-related. The letter referred to information that a WCB adjudicator had received from the complainant’s employer. The complainant had not made a direct claim from the WCB, and believed that the information given by her employer was not relevant to the actual disability. She therefore believed that her employer’s disclosures, made without her knowledge and consent, were inappropriate and unjustified.

The investigation established that her employer notified the WCB of an alleged work-related disablement and initiated a claim for compensation on the complainant’s behalf. A WCB adjudicator obtained a copy of the complainant’s original medical form and questioned the employer regarding the disablement. The employer’s representative, a human resources coordinator, confirmed that the complainant had previously missed work for a similar reason. She stated that she believed the previous absence had been due to personal, not work-related, reasons. She could not say, however, whether the current absence was work-related or not.

Regarding the collection of medical information, the company contended that its request for specific diagnoses was necessary to manage both a short- and long-term disability plan for employees. Eligibility for benefits under the long-term plan is determined on the basis of short-term benefits drawn over a certain number of days for the same disablement.

The employer noted that its purposes for collecting the information are identified on its short-term disability policy and on its medical form. It maintained that the collection of information was limited to what was necessary for these identified purposes. Furthermore,

the company noted that since the medical form contains a consent statement and is signed by the employee, employee consent is being obtained.

As for the disclosures to the WCB, the company pointed out that these were not only appropriate, but required by provincial workers' compensation legislation to which the company is subject. The legislation requires that subscribers immediately notify the WCB of any work-related disablement or allegation of such. It also authorizes the WCB to make inquiries about claims and obligates subscribers to respond to such inquiries.

Actions taken by the OPC

We determined that the company's purposes for collecting diagnostic information, namely, to manage the disability program for employees, were reasonable and legitimate. We also found that these purposes were appropriately identified, that the collection was limited to what was necessary for the fulfillment of the purposes, and that the individual's consent was obtained.

With respect to the disclosure, which was clearly done without the complainant's knowledge or consent, we determined that the disclosures in question had been required by legislation and therefore allowed under a paragraph in *PIPEDA* that provides for disclosure without knowledge or consent if it is required by law.

We concluded that these complaints were not well-founded. Nevertheless, during the investigation, it was noted that the company lacked policy, procedures, guidelines, and staff training materials relating to employee information. It was therefore recommended that the company implement appropriate policies and practices, specific to the handling of employee personal information, in accordance with the accountability principles set out in *PIPEDA*.

The Office is currently following-up with the organization to ensure that recommendations have been implemented.

Diagnosis: Reasonable in the circumstances

Overview

An employee who wanted to be accommodated in another position for medical reasons felt that his employer was attempting to collect too much information from him. When he went on leave, his employer asked him to authorize his doctor to fill out a form indicating his prognosis, limitations, treatments and abilities. The doctor provided a diagnosis and information about treatment, but did not fill out the portion concerning limitations or

abilities. The doctor provided three similar reports over a period of time, all indicating that the prognosis was unknown.

Eventually, the doctor cleared the complainant to return to work on a part-time basis. The doctor supported the complainant's request that he be transferred to a different work environment. The complainant wanted operational duties, as opposed to office ones.

But the company had not received a request from him to this effect. So the occupational health services nurse asked the doctor for more information about the medical condition. She also wanted to know whether the complainant was able to do physical work since he had been injured some years prior, which had resulted in him being transferred to an office job.

The complainant then made a formal request for a transfer on medical grounds. The company wanted additional medical information. It also indicated that an independent medical evaluation might be required. When the company refused the complainant's request, his doctor wrote to the employer in support of the complainant. The company replied that it wanted to consult a specialist before reconsidering the request. The complainant and his union objected, arguing that the company should accept the medical evaluations of the complainant's physician. In the end, the complainant returned to his desk job.

The company had a formal policy on extended sick leave. Under this policy, the employee was requested to sign a consent form authorizing the physician to disclose medical information related to the employee's illness to the company's occupational health professionals and to discuss the matter directly with them. The form contained the purposes for collecting the information – namely, consideration for eligibility benefits and establishment of fitness to work. The form asked for information about the employee's medical condition, treatment and prognosis, including diagnosis.

The company's occupational health services staff were the only employees to see this information. They were bound by their respective codes of conduct to maintain confidentiality. They provided managers only with information relating to the abilities and limitations of the employee. Detailed information about the company's policy was available to all employees via the company intranet and in a brochure.

The company also had policies and procedures in place to safeguard employee medical information. Such information was kept in a file separate from the personnel file, and stored in secure areas. Computerized information was also protected.

Actions taken by the OPC

We determined that, in light of the company's liability to continue paying the complainant during the first six months of his absence and its obligations under Canadian human rights legislation to accommodate employees with disabilities, the purposes for collecting diagnoses were legitimate and appropriate.

In considering how well the company limited its collection of personal information, we noted that the guidelines of the Canadian Human Rights Commission indicate that an employer has the right under the *Canadian Human Rights Act* to seek enough information to determine if it has an obligation to accommodate an individual with a disability and that this may involve consultation with a medical specialist. We were satisfied that the medical documentation that the employer was seeking was clearly linked to the company's obligations to accommodate the complainant and was not excessive.

We were also satisfied that the company had appropriate policies and procedures in place that outlined the purposes for collecting health information, how it is handled and by whom, and the respective roles of the employer, employee and the health services department. This information was also made available to employees in a variety of formats, thus satisfying the company's obligations under *PIPEDA* to not collect personal information indiscriminately, and to specify the type of information collected as part of their information-handling policies and practices.

We therefore concluded that this complaint was not well-founded.

Summary of the Office's position to date on employee medical information

Employers collect employee medical information for a number of reasons. Such reasons must be appropriate and legitimate in the circumstances and must be clearly identified. The information collected must be limited to these purposes.

By far, the most contentious issue raised by employees in past year was the requirement to provide diagnoses. In cases where diagnostic information was sought, our Office recognized that an employer may need to collect such information in certain limited circumstances. Thus far, we acknowledge that it may be needed to determine an employee's fitness to work and to accommodate an employee with a disability. It may also be required to determine an employee's eligibility for benefits. The Office, however, did not consider it reasonable to require a diagnosis in the case of suspicious absences or when an employee had exhausted uncertified sick leave.

The Office was clear that employee medical information, especially diagnostic information, must be handled with strict safeguards in place. Specifically, medical information must be kept separate from the employee's personnel file, in a secure location. Where diagnostic information is provided, it should only be handled by qualified medical personnel, not human resources specialists. Managers should only be provided with limited information, such as the expected date of return. Supervisors do not generally need, as a matter of course, the specifics of the employee's illness.

Such measures, of course, speak to the need for clear policies and procedures. Under *PIPEDA*, organizations are required to establish and make available policies and procedures for the handling of personal information in their care.

It should also be noted that there may be other pieces of legislation, such as labour law, workers' compensation, or human rights laws, that have a bearing on the amount of information collected, used or disclosed by the employer.

The bottom line? Organizations must ensure that they:

- only collect employee medical information for reasonable purposes;
- identify these purposes;
- obtain meaningful consent; and
- limit their collection, use, and disclosure practices to these purposes.

Incidents under *PIPEDA*

The Office also conducted thirteen incident investigations. Incidents are matters that this Office learns of from various sources including the media and organizations which have themselves identified a problem. Usually a victim is not identified and a complaint has not been filed with the Office.

Dumpster disclosures

Through media reports, our Office learned that police had found the financial records of bank customers in a suspect's apartment. The man allegedly obtained the documents from dumpsters at branches of three banks.

Representatives from the three banks retrieved the documents, and analyzed them with a view to determining their origin, identifying affected customers, and taking the appropriate corrective action.

The first bank identified the personal information of 40 customers from seven branches. It determined that the documents were likely retrieved from the garbage. While the bank has a policy with regard to the destruction of personal information, garbage disposal arrangements vary from branch to branch. Some branches contract an outside shredding service, while others require staff to physically destroy documents, either by shredding or manually ripping up, before disposal.

The bank checked the accounts, and notified all affected customers by telephone that no unusual activity had been detected. It committed to continue monitoring their account activity and asked the affected customers to do the same. The bank also gave customers the option of closing their existing accounts and opening new ones. The bank reissued its policy and procedures on the disposal of personal information, and branches were advised to reiterate the policy and procedures to staff. The bank is considering a nation-wide supplier program for locked bins and regular destruction of confidential documents.

With respect to the second bank involved, the personal information of 44 customers was retrieved. The bank concluded that the documents were taken from internal and external garbage bins as well as internal recycling and shredding receptacles. Branches have receptacles at each desk and teller wicket, which are emptied into a confidential shredding bin on a daily basis.

The bank contacted all affected customers by telephone and in writing, informing them about the ongoing police investigation. The bank offered specific advice and extra protection according to the level of risk for identity theft that their situation presented. It also advised them to monitor their accounts for unusual activity, report any missing mail, and properly safeguard their financial records. The bank issued a reminder to branch staff in the affected region regarding the proper garbage disposal policies. The policy is to be reviewed by branch staff monthly. In addition, customer garbage receptacles have been removed and only built-in wall receptacles will be used.

With respect to the third bank, 575 customers in the area were affected. Four reports were recovered that contained multiple customer names, accounting for 438 of these customers. The personal information of the remaining customers was found in a variety of documents that pertained to individual customers.

The bank believed that some of the documents were taken from the garbage as they were soiled or manually shredded. Other documents were in good condition, and the bank was unable to conclusively determine whether they came from the garbage or whether the suspect stole them from shredding boxes inside the branch. These boxes are unlocked and located close to financial and business advisor workstations.

The affected customers were grouped according to whether the information disclosed about them placed them at higher, moderate or lower risk of identity theft and fraud. Branch representatives contacted customers by telephone and told them what specific information had been disclosed. The bank invited customers in the higher and moderate risk categories to meet with a branch representative in order to review their accounts for unusual activity and open new accounts. The bank also advised them to contact their credit bureaus or HRDC if a document containing their SIN was disclosed to mitigate the risk. The bank told all customers to monitor their account activity.

The bank reviewed proper procedures with the managers of the four affected branches. It also commissioned a working group to review branch procedures and practices for the destruction of confidential records and to recommend any required changes.

This incident yielded no complaints to our Office from affected individuals.

Bank computers containing client personal information sold

The media reported on a story about a computer re-seller who had purchased two computers from a bank and then posted them on an online auction site only to discover that the computers contained the personal financial information of the bank's customers. He subsequently contacted the bank.

It turned out that when the re-seller had gone to collect the computers he had bought, an employee of the company contracted to wipe off and dispose of the bank's computer equipment inadvertently took the two computers from a pallet of servers that had not yet been cleaned.

The bank identified 350 customers whose personal information was on one or both of the computers. A variety of personal financial information was found. The bank contacted the affected customers by telephone and participated in news media interviews to convey its message that the situation was under control and that customer accounts were secure. The bank also audited the contractor involved and identified a number of gaps. The bank reviewed the disposal process and drafted a new disposal guideline.

Our Office received no complaints from affected individuals regarding this incident.

Inquiries

The Office responds to thousands of inquiries from the general public and organizations seeking advice and assistance on issues about privacy in the private sector.

The majority of calls and correspondence during the last half of 2003 concerning *PIPEDA* were from businesses, large and small, that required guidance in gearing up for the implementation of the *Act* on January 1, 2004.

We also heard from individuals who called or wrote to express dissatisfaction with organizations, claiming that they either mismanaged their personal information in some way, refused them access to or corrections of their personal information, or did not have appropriate safeguards to protect personal information.

Inquiry statistics

(January 1 to December 31, 2003)

Telephone inquiries received	9,288
Written inquiries received (letter, e-mail and fax)	4,134
Total number of inquiries received	13,422

PRIVACY PRACTICES AND REVIEWS

Audits and Compliance Reviews under the *Personal Information and Electronics Document Act (PIPEDA)*

The Office’s mandate to conduct audits of private sector organizations is derived from section 18(1) of *PIPEDA*. The *Personal Information Protection and Electronic Documents Act (PIPEDA)* enables the Commissioner to audit the compliance of private sector organizations if there are reasonable grounds to believe they are in contravention of the *Act*. Under *PIPEDA* the Commissioner may only undertake such an audit where there are “reasonable grounds” to believe that an organization is contravening a provision of the *Act*.

To date, no compliance audit of a private sector organization has been undertaken by the Office pursuant to section 18(1) of *PIPEDA*. Such evidence of non-compliance with *PIPEDA* that has come to the Office’s attention has been through complaints and

inquiries. Most of the compliance issues brought to our attention deal with discrete incidents that lend themselves to remedy within the framework of the complaint and inquiry processes.

That said, in the upcoming year our Office plans to review completed investigations under *PIPEDA* to follow-up on those well-founded complaints where remedial action was recommended. The aim of this exercise will be to determine whether recommendations made by the Commissioner are being adopted. It is expected that this will be accomplished through correspondence. The Office will conduct further inquiries where there is evidence of non-compliance.

IN THE COURTS

Under section 14 of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, an individual complainant has a right, following the Commissioner's investigation and report, to apply to the Federal Court of Canada for a hearing in respect of any matter referred to in the Commissioner's report. These matters must be among those clauses and sections of *PIPEDA* listed in section 14. Under section 14 the Commissioner may also apply directly to the Federal Court in respect of a Commissioner-initiated complaint.

Section 15 of the *Act* also allows the Commissioner to apply to appear in Federal Court in the circumstances described below. The Commissioner may, with the consent of the complainant, apply directly to the court for a hearing in respect of any matter covered by section 14; appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or, with the leave of the Court, appear as a party to any section 14 hearing.

Between January 1, 2001 and December 31, 2003 there were 20 Applications filed in Federal Court in relation to *PIPEDA*. The majority of these were discontinued, dismissed or settled prior to any pronouncement by the Court. Following are a selection of *PIPEDA* applications which raised issues of interest.

Mathew Englander v. Telus Communications Inc. and Privacy Commissioner of Canada

Federal Court Files No. T-1717-01 and A-388-03

Complaint

Mr. Englander argued that Telus uses and discloses customers' names, addresses and telephone numbers in its white pages directories and otherwise, without customers' knowledge and consent, as well as inappropriately charging customers for choosing to have their telephone number "non-published". He claimed that these actions by Telus contravene subsections 5(1) and (3) of the *Act*, as well as several clauses of Schedule 1 of the *Act*.

On the question of consent, the Commissioner found that the company did obtain valid consent through implication and was in compliance with the regulations regarding publicly available information. He focused on the company's questioning of customers regarding how their information should appear in the white-pages directory and determined that the question itself implied the eventual appearance of the information in publicly available directories. Since information subsequently published in other formats merely reflects what is published in the white pages directory, it too is considered publicly-available information for purposes of the regulations under the *Act* and may be collected, used or disclosed without consent.

As to charging fees for the non-publication of customers' information, the Commissioner noted CRTC Telecom Order 98-109, which states that telecommunications companies can charge no more than \$2.00 per month for non-published telephone service. He determined therefore that the company in question did have the authority to charge its monthly fee of \$2.00 for non-publication, and that doing so was not unreasonable.

OPC involvement

The Privacy Commissioner was granted leave to intervene in the appeal on the issues that: (1) according deference to the finding of the Privacy Commissioner and (2) the jurisdiction of the CRTC to make privacy related Orders does not restrict the Federal Court's jurisdiction under *PIPEDA*.

Court status

This was the first application for judicial review to be filed in the Federal Court under *PIPEDA*. The Application was dismissed in June 2003 at the Federal Court level.

Mr. Englander filed an appeal in the Federal Court of Appeal on 28 August 2003. No hearing date has yet been set.

Ronald G. Maheu v. IMS Health Canada et al.

Federal Court Files No. T-1967-01 and A-31-03

Complaint

Mr. Maheu complained that IMS Health Canada was improperly disclosing personal information by selling data on physicians' prescribing patterns without the consent of the physicians.

The Commissioner focused on the question of whether the information was personal information within the meaning, scope and purpose of *PIPEDA* and found that "personal information" is not so broad as to encompass all information associated with an individual. Based on this interpretation, the Commissioner found that prescription information, whether in the form of an individual prescription or in the form of patterns discerned from many prescriptions, is not personal information about a physician. Instead, he conceptualized this information as being about the professional process that led to the issuance of the prescription and concluded it must therefore be understood as work product.

OPC involvement

The Commissioner submitted written arguments on the original Application. These arguments focused only on according deference to the Privacy Commissioner and took no position as to the appropriate outcome on the facts.

The Commissioner was also involved with the procedural appeal, appearing in order to assist the Court with respect to the proper interpretation of *PIPEDA*. The Commissioner explained that an individual may file a complaint concerning an organization's information practices regardless of whether that organization collects, uses or discloses personal information about the individual complainant.

Court status

Mr. Maheu applied for a hearing in the Federal Court in November 2001.

IMS brought a motion seeking either to strike out the Application on the grounds that it was brought for an improper purpose or to have Mr. Maheu post security for costs. The Court ordered Mr. Maheu to post security for costs in the amount of \$12,000 and noted that there appeared to be reason to believe that Mr. Maheu was using the *Act* for a collateral and improper purpose given that his own personal information was not at issue. The Federal Court granted Mr. Maheu's appeal of this Order in January 2003. This decision was appealed in turn by IMS but after a hearing in November 2003 that appeal was dismissed.

The original Application in the Trial Division was discontinued in March 2004 as part of a settlement reached between Mr. Maheu and IMS.

Diane L'Écuyer v. Aéroports de Montréal and Privacy Commissioner of Canada

Federal Court Files No. T-2228-01 and A-259-03

Complaint

Madame L'Écuyer had submitted requests for access to information held by her employer. The employer refused her requests by letter, and copied the letter to three other persons – two union representatives and the coordinator of employee relations at the airport. Accordingly, she filed a complaint that her employer had, without her consent, disclosed her personal information to third parties.

Regarding the disclosure to the union representatives, the Privacy Commissioner was of the opinion that there could be implied consent for the employer to copy those parties only if the complainant had indicated that they had been copied on the original access requests. The Commissioner found that in this case no such implied consent existed, and that a reasonable person would have considered the disclosure to the union representatives to be unacceptable.

As for the employee relations coordinator, the Commissioner took note of the direct involvement of the individual in these access requests and therefore determined that it

had been appropriate for the employer to inform him of its decision to refuse access. This portion of the complaint was therefore considered to be not well founded.

OPC involvement

The Commissioner applied for and was granted leave to intervene in the appeal. In November 2003 the Commissioner submitted a factum arguing that: (1) both the Commissioner and the Court have the jurisdiction to consider privacy issues notwithstanding the fact that they are work-related; and (2) while implied consent may be appropriate in some union-involved complaints, it was not in this one and therefore the consent of the Applicant to the use and disclosure of her personal information was required.

Court status

Madame L'Écuyer filed her original Application in Federal Court in December 2001 asking that the organization correct its practices to conform with *PIPEDA*. The Privacy Commissioner was not involved in this Application. In May 2003 a decision was released, with the Court finding that the issue arose from the administration of a collective agreement and therefore was not within the jurisdiction of the Court or the Privacy Commissioner.

Madame L'Écuyer filed an appeal on 5 June 2003. The appeal was heard in June 2004 and was dismissed on the facts. The Court confirmed the trial finding the Mme. L'Écuyer had consented, at least implicitly, to the disclosure in question. The Court found it unnecessary to address the jurisdictional aspects of the appeal.

Privacy Commissioner of Canada v. Aéroports de Montréal

Federal Court File T-336-02

Complaint

An employee of an airport filed two separate complaints to the effect that her employer had refused several requests she had made for access to her personal information. In refusing access, the airport management cited two exceptions provided under *PIPEDA*, specifically s. 9(3)(a) solicitor client privilege and s. 9(3)(d) information generated in the course of a dispute resolution process.

With regard to s. 9(3)(a), the Commissioner noted that the complainant had not requested access to any lawyer's file, but rather to documents related to complaints and disciplinary measures concerning herself. He determined that the airport management had not been justified in invoking solicitor-client privilege to protect the information simply on the grounds that it had been gathered to respond to complaints and grievances or that lawyers had been consulted on the various files.

With regard to s. 9(3)(d), the Commissioner noted that the purpose of this exception is not to protect information gathered in the course of administrative processes for resolving complaints or grievances. In the Commissioner's view, a formal dispute resolution process implies the desire of parties to meet for the purpose of negotiating a resolution acceptable to each, which was not the case with the parties in question. Hence, he did not accept the employer's interpretation that the process was one of formal dispute resolution or that the information at issue had been gathered strictly for that purpose. He determined that the employer had been wrong in applying section 9(3)(d) to refuse the complainant access to her personal information.

OPC involvement

When airport management persisted with their refusal to provide access even after the Commissioner's report was issued, the Privacy Commissioner obtained the complainant's consent as required by s. 15 of *PIPEDA* and filed an Application in Federal Court.

Court status

The Aéroports, in the course of litigation, agreed with the Privacy Commissioner that the individual should be granted access to her personal information and released to the complainant all the available information to which she was entitled under *PIPEDA*. Accordingly, the Commissioner discontinued the Application in April of 2002.

Erwin Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada

Federal Court File No. T-309-03

Complaint

Mr. Eastmond complained that his employer was collecting the personal information of employees without their consent. Specifically, he was concerned that digital video recording cameras installed at the company yard could collect personal information of employees.

In making his determination, the Privacy Commissioner applied s. 5(3) and explained that when using this section one must consider both the appropriateness of the organization's purposes for collection and the circumstances surrounding those purposes. To that end, he fashioned a four-point test for assessing reasonableness, namely: (1) is the measure demonstrably necessary to meet a specific need? (2) Is it likely to be effective in meeting that need? (3) Is the loss of privacy proportional to the benefit gained? and (4) Is there a less privacy-invasive way of achieving the same end? Considering the company's stated purposes against this backdrop, the Privacy Commissioner did not believe that a reasonable person would consider these circumstances to warrant such an intrusive measure as digital video surveillance. As such, he concluded that the company's use of this type of surveillance for their stated purposes was not appropriate and that the company had contravened s. 5(3) of *PIPEDA*.

OPC involvement

The Privacy Commissioner was added as a party pursuant to s. 15(c) of *PIPEDA*, however she took no position as to the appropriate outcome on the merits. Instead, she argued that the Court should accord some deference to the expertise of the Privacy Commissioner and should adopt the four-point test to determine the appropriateness of the collection of the information by CP Rail. A supplementary factum was filed in December 2003 addressing both the Privacy Commissioner and Court's jurisdiction over the issues, notwithstanding that they arose in a collective bargaining employment situation.

Court status

Mr. Eastmond filed an Application in Federal Court in February 2003. Among other things, the Application requested that the Privacy Commissioner send a certified copy of the Commissioner's Record of investigation to the Applicant and to the Registry. Upon objection on behalf of the Privacy Commissioner to this request, the Court decided in June 2003 that the *Federal Court Rules* do not allow an Applicant to request material in the possession of the Privacy Commissioner.

The Application was heard in April 2004 and on 11 June 2004 the court released its decision. On the question of jurisdiction, the Court found that the Privacy Commissioner did have jurisdiction, the essence of this dispute did not arise from the collective agreement, and that it was not Parliament's intention to exclude unionized workers from the scope of *PIPEDA*. On the question of deference it was established that although this was a proceeding *de novo*, the Privacy Commissioner was entitled to a degree of deference in light of her expertise. Finally, the court adopted the Commissioner's four-point test for s. 5(3), with the caveat that the specific factors considered in this case might not be appropriate in all cases. Using that test, the court concluded that a reasonable person would consider the organization's purposes for collecting the images through the medium of a digital video camera to be appropriate in the circumstances, and therefore that CP Rail had not contravened *PIPEDA*.

Robert Lavigne v. Canadian Union of Postal Workers

Federal Court File No. T-500-03

Complaint

After determining that day and month of birth was being used as a seniority "tie-breaker", Mr. Lavigne complained that CUPW was using his personal information in a way that was inconsistent with the purposes for which the information was originally collected. The Office determined that it did not have jurisdiction to accept Mr. Lavigne's complaint because CUPW was neither a federal work, undertaking or business nor was there disclosure across borders for consideration.

OPC involvement

The Privacy Commissioner was not formally involved in the proceeding. However, the Application raised interesting procedural issues about what constituted a “complaint” for the purposes of s. 13 and 14.

Court status

Although no complaint was accepted and no Commissioner’s report issued, Mr. Lavigne filed a section 14 Application in Court, asking the Court to rule on the merits of the complaint and seeking damages from CUPW. CUPW brought a motion to strike the Application while Mr. Lavigne sought leave to convert the Application into an action. The Federal Court granted CUPW’s motion and the Application was struck in August 2003 with costs to the Respondent.

Yukon Hospital Corporation v. Privacy Commissioner of Canada

Federal Court File T-1451-03

Complaint

The Office of the Privacy Commissioner received a complaint from an employee alleging that the Whitehorse General Hospital had refused a request for access to her personal information in its possession. The Hospital was accordingly notified that a complaint had been received and that an investigation was being commenced.

The Hospital took the position that in order for *PIPEDA* to apply, the hospital must either engage in commercial activities or operate a federal work, undertaking or business. It was their opinion that neither of these applied, and therefore that the hospital was not subject to *PIPEDA*. In contrast, the Commissioner took the position that intra-territorial enterprises in the three territories fall within the definition of “federal work, undertaking or business” by virtue of s. 2(1) definition of “federal work, undertaking or business”, specifically subsection (i) “outside the exclusive legislative authority of the legislatures of the provinces” and thus that employees of organizations such as the Whitehorse General Hospital fall within the jurisdiction of *PIPEDA*. As such, the Office intended to continue with its statutorily mandated investigation.

OPC involvement

The Commissioner was required to respond to the judicial review application directed at the Office's assertion of jurisdiction.

Court status

The Hospital filed an Application under s. 18.1 of the *Federal Court Act*, requesting judicial review of the Privacy Commissioner's decision that the Whitehorse General Hospital was subject to *PIPEDA* and the subsequent decision to proceed with an investigation.

Ultimately, the complainant reached a settlement with the Hospital, part of which was the withdrawal of her complaints to the Office of the Privacy Commissioner. When her complaints were withdrawn, the Application for judicial review was formally discontinued in February 2004.

Blood Tribe Department of Health v. Privacy Commissioner of Canada

Federal Court File No. T-2222-03

Complaint

A complaint was filed with the Office of the Privacy Commissioner alleging (among other things) that the Blood Tribe Department of Health denied an individual access to her personal information and did not provide reasons for the denial. Although the Commissioner needs access to all documents in order to ensure that exemptions claimed have been properly applied and to guard against abuse, in the course of the investigation, the Blood Tribe Department of Health refused to provide the Privacy Commissioner with access to solicitor-client privileged documents. As a result of the refusal, the Office of the Privacy Commissioner issued an Order for the production of records pursuant to sections 12(1)(a) and (c) of *PIPEDA*.

OPC involvement

The Commissioner was required to respond to the judicial review application directed at the Office's assertion of jurisdiction.

Court status

The Blood Tribe Department of Health filed an Application for judicial review, under s. 18.1 of the *Federal Court Act*, of the decision of the Office to issue the Order for production. The Application was filed in Federal Court in October 2003 but incorrectly named the Respondent. The Notice of Application has been amended and was properly served on 3 June 2004. The Application is now progressing normally.

Canada (Attorney General) v. Canada (Information Commissioner), 2004 FC 431, [2004] F.C.J. No. 524

Although the Privacy Commissioner was not involved in the following proceedings, this was an important decision for the Office given that both the Information and Privacy Commissioners have the same investigative powers set out under their parallel Acts.

In March 2004 the Federal Court dismissed 25 applications for judicial review which had been filed by the government in an attempt to limit the investigative powers of the Information Commissioner.

The government had challenged the Information Commissioner's authority to investigate, arguing that the Prime Minister's Office and Ministerial offices are separate and distinct from the Privy Council Office or a Minister's department. The Court found that it was premature to rule on whether the records were subject to the *Act* and that the Commissioner should have been allowed to complete his investigation and report before such issues were raised. In so finding, the Court recognized the importance of the Commissioner's investigative role and independent review where rights of access are in dispute.

The government has appealed only one narrow legal point of the ruling dealing with whether the Information Commissioner has the right to see a legal memorandum.

PART THREE

Corporate Services

Our path toward institutional renewal

It has been a challenging year for our Office due to the chain of events surrounding the resignation of the former Commissioner in June, 2003. A Parliamentary Committee inquiry, Auditor-General's report, a Public Service Commission investigation and numerous internal reviews and audits took time and energy from normal office functions. These audits and reviews highlighted that there had been a major breakdown of external governance and internal control processes at the OPC. In response, our Office has taken substantial steps to rebuild and renew the agency.

A series of corrective measures have been and continue to be taken to improve our office management framework and processes. These include:

- The appointment of two Assistant Commissioners and a Chief Financial Officer
- The establishment of an External Advisory committee of national privacy experts
- A Modern Comptrollership action plan has been submitted to Treasury Board
- Training in financial management policies, as well as Values and Ethics, has been provided to managers and staff
- Appointment of the Assistant Commissioner as OPC Values & Ethics Champion
- Development of a Human Resources strategy and action plan has been developed
- The establishment of Health & Safety and union-management consultation committees
- A Canada School of Public Service learning program is being implemented for staff

An important part of our internal renewal was the strategic planning process that was launched in January 2004. This was a transparent planning exercise with considerable

staff involvement. The process established an overall framework for the development of OPC strategies, and key actions for the fiscal year 2004-2005. The resulting strategic framework formed the basis of our Report on Plans and Priorities, which was submitted to Treasury Board in April.

One of the key strategic outcomes identified by senior staff in the strategic planning exercise for the OPC is, *"To be a well-managed, effective and efficient Parliamentary agency"*. The development and implementation of a modern comptrollership plan is at the heart of the OPC achieving this objective. The Modern Comptrollership Action Plan that was completed, and submitted to Treasury Board in March will help us ensure that adequate management processes and controls are in place, providing a strong foundation for the Office's activities. Regular communication to staff on Modern Comptrollership and status reports to senior management will instil a modern comptrollership culture, and ensure that modern comptrollership-related principles and practices are followed.

The Modern Comptrollership framework for the Office includes a strong human resources focus. Key elements include shared values and ethics — and motivated staff. We are placing emphasis on these important aspects of the modern comptrollership framework as part of the overall renewal of the OPC.

Some of the other major corporate services accomplishments in 2003-2004 were:

- Launch of Integrated Investigation Application (IIA), an integrated caseload management system that supports key business processes.
- Completion of an Information Technology (IT) threat and risk analysis looking at issues such as security and IT operations. Many of the recommendations highlighted in this analysis, including those specifically relating to the integration of the external and internal networks, have been implemented.
- Completion and roll out of a revised delegation of financial authority framework.
- Provision of training to OPC staff on important financial policies, such as delegation, travel and hospitality.
- Development of an accommodation strategy for OPC.
- Enhancement of controls in the contracting process.

In FY 2004-05 the Corporate Services group will be focusing on initiatives in areas such as performance measurement, the streamlining of business processes, and human resources planning and management within the OPC.

At the beginning of fiscal year 2003-2004, the Office's budget was \$11.2 million, the same as our budget of the previous year. Included in our budget was \$6.7 million for the Office's *PIPEDA* activities. Funding of OPC activities has been and continues to be an important issue.

Initially, *PIPEDA* funding was provided for a three year period ending March 31, 2004, to allow the OPC to administer the new *Act*. This *Act* first came into force for certain sectors, specifically federally-regulated business, in January 2001. As of January 2004, however, the scope of the *Act* has increased to include the entire private sector. When funding was provided for the first three years of *PIPEDA*, the expectation was that towards the end of the three year period the Office would evaluate its experience in undertaking *PIPEDA*-related activities, and would confirm with Treasury Board its on-going funding requirements for this work.

Unfortunately, as a result of the events of FY 2003-2004 relating to the resignation of the former Commissioner, we were unable to perform this review with Treasury Board. At the end of fiscal 2003-2004, we obtained one year bridge funding for the OPC *PIPEDA*-related activities for fiscal 2004-2005. The Office is currently reviewing its financial resources, and plans to make a submission to Treasury Board in the fall of 2004 for on-going funding under both the *Privacy Act* and *PIPEDA*.

Resources

April 1, 2003 to March 31, 2004

	Expenditure Totals (\$)	% of Totals
<i>Privacy Act</i>	4,171,661	37.61 %
<i>PIPED Act</i>	4,768,650	42.99 %
Corporate Services	2,151,980	19.40 %
Total	11,092,291	100.00 %

Note that as of March 2004 there were 95 full time staff positions at the Office of the Privacy Commissioner of Canada

Detailed Expenditures ⁽¹⁾	Privacy Act	PIPED Act	Corporate Services	Total
Salaries	3,605,276	3,176,545	401,153	7,182,974
Employee Benefits Program	198,097	878,851	160,870	1,237,818
Transportation & Communication	108,074	93,266	238,789	440,129
Information	70,366	80,773	76,088	227,227
Professional Services	191,986	385,886	588,181	1,166,053
Rentals	16,328		82,277	98,605
Repairs & Maintenance			291,026	291,026
Materials & Supplies	8,613	3,330	82,454	95,397
Acquisition of Machinery & Equipment		150,000	230,985	380,985
Other Subsidies & Payments	-27,079		156	(26,923)
Total	\$4,171,661	\$4,768,651	\$2,151,979	\$11,092,291

⁽¹⁾ Total expenditure figures are consistent with the public accounts.

Financial statements

Over the past several years, as part of the Financial Information Strategy, the Receiver General for Canada and departments have worked to put in place new financial information systems and to acquire the accounting expertise required to implement full accrual accounting. Overseeing this initiative, the Treasury Board Secretariat also developed the necessary accounting policies and training programs to implement full accrual accounting government-wide.

Under full accrual accounting, an entity's financial statements provide a more comprehensive and up-to-date picture of its financial situation and better reflect the impact of economic events and decisions made during the fiscal year. Better information means improved transparency and accountability.

Publication of accrual-based financial statements is being phased in for departments and agencies. Departmental corporations began presenting accrual-based financial statements in Volume II Part II of the *2001-2002 Public Accounts of Canada*. For 2003-2004, the offices of the five agents of Parliament (the Offices of the Auditor General, Chief Electoral Officer, Commissioner of Official Languages, Privacy Commissioner and Information Commissioner) will report accrual-based financial statements in accordance with generally accepted accounting principles. Information on the use of their appropriations is contained in the preceding reports presented in the following tables.

In general terms, the use of appropriations focuses on spending and the acquisition of resources. Accrual accounting reports the cost of resources consumed during the year as well as reporting the assets and future financial obligations. For further details on the adoption of full accrual accounting, please refer to Annex 6 in *The Budget Plan 2003*.

The Management Responsibility letter and the audited financial statements as at March 31, 2004 are available on our web site <http://www.privcom.gc.ca>.

Ces dernières années, dans le cadre de la Stratégie d'information financière, le receveur général du Canada et les ministères se sont appliqués à implanter de nouveaux systèmes d'information financière et à acquérir l'expertise comptable essentielle à l'adoption de la comptabilité d'exercice intégrale. Chargé de surveiller la réalisation de cette initiative, le Secrétaire du Conseil du Trésor a aussi mis au point les conventions comptables et les programmes de formation nécessaires pour instaurer la comptabilité d'exercice à l'échelle du gouvernement.

Grâce à la méthode de la comptabilité d'exercice, il est possible d'établir des états financiers qui présentent un tableau plus complet et à jour de la situation financière et reflètent davantage l'impact des événements économiques et des décisions qui ont été prises au cours de l'année financière. Une information de meilleure qualité contribue à accroître la transparence et la responsabilisation.

Les ministères et organismes vont intégrer des états financiers établis selon la méthode de la comptabilité d'exercice de façon progressive. Les établissements publics ont commencé à présenter des états financiers établis selon cette méthode à la partie II du volume II des *Comptes publics du Canada 2001-2002*. Pour 2003-2004, les bureaux des cinq agents du Parlement (vérificateur général, directeur général des élections, Commissaire aux langues officielles, Commissaire à l'information et Commissaire à la protection de la vie privée) présenteront leurs états financiers selon la comptabilité d'exercice en appliquant les principes comptables généralement reconnus. L'information sur l'utilisation de leurs crédits que contenaient les rapports précédents sur le rendement est présentée dans les tableaux qui suivent.

La présentation de renseignements sur l'utilisation des crédits est axée sur les dépenses et l'acquisition de ressources. La comptabilité d'exercice permet de présenter le coût des activités qui ont été réalisées ou les recettes qui ont été perçues au cours de l'année ainsi que les avoirs qui ont été utilisés et les obligations financières dont il faudra s'acquitter à l'avenir. Pour plus de renseignements sur l'adoption de la comptabilité d'exercice intégrale, veuillez vous reporter à l'annexe 6 du *Plan budgétaire de 2003*.

La lettre de responsabilité de la direction a l'égard des états financiers et les états financiers vérifiés en date du 31 mars 2004 peuvent être consultés sur notre site web <http://www.privcom.gc.ca>.

Ressources

Du 1^{er} avril 2003 au 31 mars 2004

Dépenses globales (\$)	% du total
Loi sur la protection des renseignements personnels	37,61 %
Loi sur la protection des renseignements personnels et les documents électroniques	42,99 %
Gestion intégrée	19,40 %
Total	100,00 %

À noter que depuis mars 2004, le Commissariat à la protection de la vie privée du Canada compte 95 employés à temps plein.

Dépenses détaillées ⁽¹⁾	Loi sur la protection des renseignements personnels	Loi sur la protection des renseignements personnels et les documents électroniques	Gestion intégrée	Total
Salaires et traitements	3 605 276	3 176 545	401 153	7 182 974
Cotisations au régime d'avantages sociaux	1 98 097	878 851	160 870	1 237 818
des employés				
Transports et communications	108 074	93 266	238 789	440 129
Information	70 366	80 773	76 088	227 227
Services professionnels	191 986	385 886	588 181	1 166 053
Locations	16 328		82 277	98 605
Réparations et entretien			291 026	291 026
Approvisionnements et fournitures	8 613	3 330	82 454	95 397
Achat de machines et d'équipements		150 000	230 985	380 985
Autres subventions et paiements	-27 079		156	(26 923)
Total	4 171 661 \$	4 768 651 \$	2 151 979 \$	11 092 291 \$

⁽¹⁾ Les dépenses globales correspondent aux données des comptes publics.

- Fourniture de séances de formation aux employés du CPVP sur les politiques financières importantes comme celles sur la délégation des pouvoirs, les voyages et l'accueil.
- Élaboration d'une stratégie relative à l'hébergement pour le CPVP.
- Amélioration des contrôles du processus de passation de marchés.

Au cours de l'exercice 2004-2005, la Direction de la gestion intégrée concentrera ses efforts sur des initiatives dans des domaines tels que la mesure du rendement, la rationalisation des procédés opérationnels ainsi que la gestion et la planification des ressources humaines au CPVP.

Au début de l'exercice 2003-2004, le budget du Commissariat s'établissait à 11,2 millions de dollars, soit le même montant que celui de l'exercice précédent. De cette somme, 6,7 millions de dollars visent les activités du Commissariat à l'égard de la *LPRPDE*. Le financement des activités du CPVP est et demeure un enjeu important.

Au départ, le financement au titre de la *LPRPDE* a été fourni pour une période de trois ans se terminant le 31 mars 2004, ce qui devait permettre au CPVP d'administrer la nouvelle *Loi*. Cette *Loi* a commencé à s'appliquer à certains secteurs, notamment les entreprises sous réglementation fédérale, en janvier 2001. Toutefois, à partir de janvier 2004, la portée de la *Loi* a été élargie afin d'inclure l'ensemble du secteur privé. Lorsque le financement a été accordé pour les trois premières années de mise en œuvre de la *LPRPDE*, on s'attendait à ce qu'à la fin de cette période, le Commissariat tienne en compte l'exercice des activités liées à la *LPRPDE* et confirme auprès du Conseil du Trésor ses besoins financiers permanents pour ces travaux.

Malheureusement, en raison des événements de l'exercice 2003-2004 se rapportant à la démission de l'ancien Commissaire, nous n'avons pu mener cet examen avec le Conseil du Trésor. À la fin de 2003-2004, nous avons obtenu des fonds provisoires pour un an au titre des activités du CPVP liées à la *LPRPDE* pour l'exercice 2004-2005. À l'heure actuelle, le Commissariat se penche sur ses ressources financières et prévoit remettre un compte rendu au Conseil du Trésor à l'automne 2004 dans lequel il demandera des crédits permanents conformément à la *Loi sur la protection des renseignements personnels* et à la *LPRPDE*.

Le processus de planification stratégique, lancé en janvier 2004, représente une importante partie de notre renouvellement interne. Il s'agit d'un exercice de planification transparente exigeant une très forte participation des employés. Le processus a établi un cadre global d'élaboration des stratégies du CPVP ainsi que des mesures clés pour l'exercice 2004-2005. Le cadre stratégique qui en a résulté a servi de fondement au Rapport sur les plans et les priorités que nous avons remis au Conseil du Trésor en avril.

Dans le cadre de l'exercice de planification, la haute direction a établi des résultats stratégiques clés pour le CPVP dont celui d'« être un organisme parlementaire bien géré, efficace et efficient ». Pour ce faire, le CPVP devra principalement élaborer et mettre en œuvre un plan de modernisation de la fonction de contrôle. Le Plan d'action de la modernisation de la fonction de contrôle établi et présenté au Conseil du Trésor en mars dernier nous permettra de nous assurer que des processus et des contrôles de gestion satisfaisants sont en place et qu'ils procurent de solides assises aux activités du Commissariat. Les communications périodiques aux employés sur la modernisation de la fonction de contrôle et la présentation de rapports d'étape à la haute direction favoriseront une culture de contrôle moderne et veilleront à ce que les principes et les pratiques se rapportant à la modernisation de la fonction de contrôle soient respectés.

Le cadre de modernisation de la fonction de contrôle du Commissariat accorde une très grande importance aux ressources humaines et repose au premier plan sur des éléments tels que les valeurs et l'éthique partagées et des employés motivés. Nous mettons l'accent sur ces importants volets du cadre de modernisation de la fonction de contrôle, lequel s'inscrit dans les efforts globaux de renouvellement du CPVP.

Les autres grandes réalisations en matière de gestion intégrée en 2003-2004 sont énumérées ci-après :

- Lancement de l'Application d'enquête intégrée (AEI), un système intégré de gestion de la charge de travail qui appuie les principaux procédés opérationnels. Achèvement d'une analyse des menaces et des risques associés à la technologie de l'information (TI), qui a porté sur des éléments tels que la sécurité et les opérations de TI. Nombre des recommandations formulées dans l'analyse, dont celles se rapportant précisément à l'intégration des réseaux externes et internes, ont été mises en œuvre.
- Achèvement et mise en place d'un cadre révisé de délégation des pouvoirs financiers.

Gestion intégrée

Notre cheminement vers le renouvellement institutionnel

Cette dernière année a été éprouvante pour le Commissariat en raison de l'enchaînement des événements ayant entouré la démission de l'ancien Commissaire en juin 2003. L'enquête d'un comité parlementaire, le rapport de la vérificatrice générale, une enquête de la Commission de la fonction publique et de nombreux examens et vérifications internes ont détourné temps et énergie des fonctions de bureau normales. Ces vérifications et examens ont mis au jour une défaillance d'envergure des processus de gouvernance externe et de contrôle interne au CPVP. Le Commissariat a pris des mesures notables pour rebâtir et renouveler l'organisme.

Une série de mesures correctives ont été prises et continuent de l'être afin d'améliorer le cadre et les processus de gestion du Commissariat, dont celles qui suivent :

- la nomination de deux commissaires adjoints et d'un agent en chef des services financiers;
- la mise sur pied d'un comité consultatif externe d'experts-conseils nationaux en matière de renseignements personnels ;
- la présentation d'un plan de modernisation de la fonction de contrôleur au Conseil du Trésor;
- l'offre de séances de formation en matière de politiques de gestion financière ainsi que de valeurs et d'éthique aux gestionnaires et aux employés;
- la nomination d'un des commissaires adjoints à titre de chef de file en matière d'éthique et de valeurs du CPVP;
- l'élaboration d'une stratégie et d'un plan d'action en matière de ressources humaines;
- la mise sur pied de comités de santé et sécurité et de comités consultatifs syndicaux-patronaux;
- la mise en œuvre d'un programme d'apprentissage de l'École de la fonction publique du Canada à l'intention des employés.

Intervention du CPVP

Le Commissaire a dû donner suite à une demande de contrôle judiciaire de l'allégation de compétence du Commissariat.

État de la situation

Aux termes de l'article 18.1 de la *Loi sur les Cours fédérales*, le Blood Tribe Department of Health a déposé une demande de contrôle judiciaire de la décision du Commissaire de prendre une ordonnance de production de dossiers. La demande a été déposée à la Cour fédérale en octobre 2003, mais le nom de l'intimé contenait une erreur, de sorte que l'avis de demande a dû être modifié et présenté de manière appropriée le 3 juin 2004. La demande suit maintenant son cours normal.

Canada (Procureur général) c. Canada (Commissaire à l'information), 2004 CF 431, [2004] A.C.F. n° 524

Même si la Commissaire à la protection de la vie privée n'est pas intervenue, la procédure suivante est une importante décision pour le Commissariat étant donné que le Commissaire à l'information et la Commissaire à la protection de la vie privée disposent tous les deux des mêmes pouvoirs d'enquête en vertu des lois les régissant respectivement.

En mars 2004, la Cour fédérale a rejeté 25 demandes de contrôle judiciaire que le gouvernement avait déposées afin de limiter les pouvoirs d'enquête du Commissaire à l'information.

Le gouvernement a contesté le pouvoir d'enquêter du Commissaire à l'information et prétendu que le Cabinet du Premier ministre et les cabinets des ministres étaient distincts du Bureau du Conseil privé et du ministère d'un ministre. La Cour a conclu qu'il était trop tôt pour statuer sur l'assujettissement des dossiers à la *Loi* et que le Commissaire à l'information aurait dû pouvoir terminer son enquête et présenter son rapport avant que ces questions ne soient soulevées. En présentant une telle conclusion, la Cour a reconnu l'importance du rôle d'enquêteur du Commissaire et des examens indépendants lorsque les droits d'accès sont contestés.

Le gouvernement a porté appel d'un point légal limité de la décision portant sur la question de savoir si le Commissaire à l'information a le droit de prendre connaissance d'un mémoire juridique.

ressortissant pas au pouvoir législatif exclusif des législatures provinciales») et que, partant, les employés d'organisations telles que le Whitehorse General Hospital étaient assujettis à la *LPRPDE*. C'est pourquoi le Commissariat entend poursuivre l'enquête qu'il est habilité à mener aux termes de la loi.

Intervention du CPVP

Le Commissaire a dû donner suite à la demande de contrôle judiciaire de l'allégation de compétence du Commissariat.

État de la situation

Aux termes de l'article 18.1 de la *Loi sur les Cours fédérales*, l'hôpital a déposé une demande de contrôle judiciaire de la décision du Commissaire à la vie privée selon laquelle le Whitehorse General Hospital était assujéti à la *LPRPDE* et de sa décision ultérieure de déclencher une enquête.

La plaignante a fini par conclure une entente avec l'hôpital qui comprenait notamment le retrait de ses plaintes auprès du Commissariat à la protection de la vie privée. Au retrait des plaintes, la demande de contrôle judiciaire a été officiellement abandonnée en février 2004.

Blood Tribe Department of Health c. Commissaire à la protection de la vie privée du Canada

N° de dossier de la Cour fédérale T-2222-03

Plainte

Une plainte a été déposée auprès du Commissariat à la protection de la vie privée alléguant (entre autres choses) que le Blood Tribe Department of Health avait refusé à une personne l'accès à ses renseignements personnels sans justifier son refus. Bien que le Commissaire doive avoir accès à tous les documents pour s'assurer que les exceptions invoquées ont été bien appliquées et pour éviter les abus, dans le cadre de l'enquête, le Blood Tribe Department of Health a refusé de donner au Commissaire à la protection de la vie privée accès à des documents protégés par le secret professionnel. En raison de ce refus, le Commissariat à la protection de la vie privée a pris une ordonnance de production de dossiers conformément aux alinéas 12(1)*a*) et *c*) de la *LPRPDE*.

entreprise ou un secteur d'activité fédéral et qu'aucune communication entre frontières ne devait être soumise à un examen.

Intervention du CPVP

Le Commissaire à la protection de la vie privée n'est pas intervenu officiellement dans l'affaire, mais la demande a soulevé d'intéressantes questions procédurales concernant les éléments constitutifs d'une « plainte » en vertu des articles 13 et 14.

État de la situation

Même si aucune plainte n'a été acceptée et qu'aucun rapport du Commissaire n'a été déposé, M. Lavigne a présenté à la Cour une demande conformément à l'article 14 dans laquelle il l'enjoignait de statuer sur le fond de la plainte et d'imposer des dommages punitifs au SPC. Pour sa part, le SPC a présenté une requête en radiation de la demande alors que M. Lavigne a demandé l'autorisation de convertir la demande en un litige. La Cour fédérale a accueilli la demande du SPC et celle-ci a été radiée en août 2003 avec adjudication de frais à l'intimé.

Yukon Hospital Corporation c. Commissaire à la protection de la vie privée du Canada

N° de dossier de la Cour fédérale T-1451-03

Plainte

Le Commissariat à la protection de la vie privée a reçu une plainte d'une employée qui prétendait que le Whitehorse General Hospital avait refusé de donner suite à sa demande d'accès à ses renseignements personnels. L'hôpital a par conséquent été informé qu'une plainte avait été déposée et qu'une enquête s'amorçait.

L'hôpital a soutenu que, pour que la LPRPDÉ s'applique, il doit exercer des activités commerciales ou exploiter un ouvrage, une entreprise ou un secteur d'activité fédéral. Il était d'avis que ni l'une ni l'autre de ces conditions ne s'appliquaient et, par conséquent, que l'hôpital n'était pas assujéti à la LPRPDÉ. En revanche, le Commissaire a prétendu que les entreprises interterritoriales des trois territoires étaient visées par l'expression « entreprises fédérales » au sens du paragraphe 2(1), mais plus particulièrement de l'alinéa 2(1*i*) (« les installations, ouvrages, entreprises ou secteurs d'activité ne

du Commissaire à la protection de la vie privée et de la Cour, même si l'affaire découle d'une situation d'emploi visée par une convention collective.

État de la situation

M. Eastmond a déposé une requête à la Cour fédérale en février 2003 dans laquelle il demandait, entre autres choses, au Commissaire à la protection de la vie privée d'envoyer une copie certifiée de son rapport d'enquête au requérant et au greffe. Le Commissaire a la protection de la vie privée s'étant opposé à donner suite à cette demande, la Cour a décidé en juin 2003 que les *Règles de la Cour fédérale* ne permettaient pas à un demandeur d'exiger du matériel en la possession du Commissaire à la protection de la vie privée.

La requête a été entendue en avril 2004 et, le 11 juin 2004, la Cour a fait connaître sa décision. Au sujet de la compétence, la Cour a conclu que le Commissaire à la protection de la vie privée avait compétence en la matière, que l'essentiel du litige ne découlait pas de la convention collective et que le Parlement n'avait pas l'intention d'exclure les syndiqués du champ d'application de la *LPRPD*. Au sujet de la retenue judiciaire, elle a établi que, même s'il s'agissait d'une procédure *de novo*, le Commissaire à la protection de la vie privée avait droit à une certaine retenue compte tenu de son expertise. Enfin, la Cour a adopté les quatre critères proposés par le Commissaire concernant le paragraphe 5(3) en précisant que les facteurs particuliers pris en compte en l'espèce pourraient ne pas s'appliquer dans toutes les affaires. En se servant de ces critères, la Cour a conclu qu'une personne raisonnable estimerait que les fins invoquées par l'organisation pour recueillir les images par l'entremise d'une caméra vidéo numérique sont appropriées dans les circonstances et, par conséquent, la Compagnie de chemin de fer Canadien Pacifique n'a pas enfreint la *LPRPD*.

Robert Lavigne c. Syndicat des postiers du Canada

N° de dossier de la Cour fédérale T-500-03

Plainte

Lorsqu'il a appris que la date de naissance avait servi à rompre l'égalité pour établir une priorité basée sur l'ancienneté, M. Lavigne s'est plaint que le SPC se servait de ses renseignements personnels d'une manière non conforme aux fins pour lesquelles ils avaient été recueillis initialement. Le Commissariat a établi qu'il n'avait pas la compétence voulue pour accepter la plainte de M. Lavigne parce que le SPC n'est pas un ouvrage, une

Erwin Eastmond c. Compagnie de chemin de fer Canadien Pacifique et le Commissaire à la protection de la vie privée du Canada

N° de dossier de la Cour fédérale T-309-03

Plainte

M. Eastmond s'est plaint que son employeur recueillait des renseignements personnels sur ses employés sans leur consentement. Le plaignant était surtout préoccupé par le fait que des caméras d'enregistrement vidéo numériques installées dans la cour de la compagnie pourraient recueillir des renseignements personnels sur les employés.

Dans le cadre de son enquête, le Commissaire à la protection de la vie privée a invoqué le paragraphe 5(3) et expliqué qu'il devait prendre en considération la pertinence des objectifs de la compagnie pour recueillir des renseignements personnels ainsi que les circonstances entourant ces objectifs. À cette fin, il a pris en compte les questions suivantes : (1) Est-il possible de faire la preuve que la mesure est nécessaire pour répondre à un besoin particulier? (2) Est-elle susceptible d'être efficace pour répondre à ce besoin? (3) L'invasion de la vie privée est-elle proportionnelle à l'avantage qui en découlera? (4) Existe-t-il un autre moyen moins envahissant qui pourrait permettre d'atteindre le même objectif? Compte tenu des fins déclarées de l'entreprise, le Commissaire à la protection de la vie privée n'a pas cru qu'une personne raisonnable prendrait en considération ces circonstances pour justifier la prise d'une mesure portant autant atteinte à la vie privée comme l'installation de caméras vidéo numériques. Par conséquent, l'utilisation de ce type de surveillance vidéo par la compagnie aux fins mentionnées n'est pas appropriée et l'entreprise contrevient au paragraphe 5(3) de la LPRPDE.

Intervention du CPVP

Le Commissaire à la protection de la vie privée a été ajouté à titre de partie en vertu de l'alinéa 15c) de la LPRPDE, mais il ne s'est pas prononcé sur l'issue ultime de l'affaire quant au fond. Il a plutôt soutenu que la Cour devrait accorder une certaine retenue judiciaire à l'expertise du Commissaire à la protection de la vie privée et adopter les quatre critères (voir les quatre questions citées précédemment) pour déterminer la pertinence de la collecte des renseignements par la Compagnie de chemin de fer Canadien Pacifique. Un autre mémoire a été déposé en décembre 2003 traitant de la compétence en la matière

dans la *LPRPDE* qui s'appliquent spécifiquement à des renseignements protégés par le secret professionnel liant l'avocat à son client (l'alinéa 9(3)a)) et à des renseignements fournis uniquement à l'occasion d'un règlement officiel des différends (l'alinéa 9(3)d)).

En ce qui concerne l'alinéa 9(3)a), le Commissaire a fait remarquer que la plaignante n'avait jamais demandé accès à un dossier d'avocat, mais plutôt à des documents liés à des plaintes et à des mesures disciplinaires la concernant. Il a jugé que la direction de l'aéroport ne pouvait pas invoquer le secret professionnel liant l'avocat à son client pour protéger les renseignements au simple motif qu'ils avaient été recueillis en réponse à des plaintes et des griefs ou que des avocats avaient été consultés relativement aux différends dossiers.

En ce qui concerne l'alinéa 9(3)d), le Commissaire a fait remarquer que cette exception n'a pas pour objet de protéger les renseignements recueillis dans le cadre de processus administratifs visant à régler des plaintes ou des griefs. À ses yeux, la notion d'un règlement officiel des différends suppose que les parties ont désiré se rencontrer pour négocier un règlement acceptable de part et d'autre — ce qui n'était pas le cas avec les parties en question. Il n'a donc pas accepté l'interprétation de l'employeur selon laquelle le processus était un règlement officiel des différends, ou encore que les renseignements en question avaient été recueillis à cette fin expresse. Il a jugé que l'employeur avait eu tort d'appliquer l'alinéa 9(3)d) pour refuser à la plaignante l'accès à ses renseignements personnels.

Intervention du CPVP

Lorsque la direction de l'aéroport a persisté dans son refus de donner accès même après le dépôt du rapport du Commissaire à la protection de la vie privée, ce dernier a obtenu le consentement de la plaignante pour porter l'affaire devant la Cour fédérale comme le stipule l'article 15 de la *LPRPDE*.

État de la situation

La direction des aéroports, pendant le litige, a convenu avec le Commissaire à la protection de la vie privée que la plaignante devait avoir accès à ses renseignements personnels et lui a communiqué tous les renseignements auxquels elle avait droit en vertu de la *LPRPDE*. Par conséquent, le Commissaire a abandonné la demande en avril 2002.

Intervention du CPVP

Le Commissaire a demandé l'autorisation d'intervenir dans l'appel et sa demande a été accordée. En novembre 2003, il a présenté un mémoire dans lequel il prétendait : (1) que le Commissaire et la Cour avaient la compétence de trancher des questions en matière de vie privée, qu'elles soient ou non liées au travail et (2) que, si le consentement implicite peut convenir dans quelques plaintes faisant intervenir les syndicats, tel n'était pas le cas en l'espèce et que, par conséquent, il fallait obtenir le consentement de la plaignante pour utiliser et communiquer ses renseignements personnels.

État de la situation

M^{me} L'Écuyer a déposé sa première demande auprès de la Cour fédérale en décembre 2001 et demandé que l'organisation rectifie ses pratiques pour les rendre conformes à la LPRPDÉ. Le Commissaire à la protection de la vie privée n'était pas partie à cette demande. En mai 2003, la Cour a rendu une décision et conclu que la question s'est posée dans le cadre de l'administration d'une convention collective et que, par conséquent, ni le Commissaire à la protection de la vie privée ni la Cour n'avaient compétence dans cette affaire.

M^{me} L'Écuyer a interjeté appel le 5 juin 2003. L'appel a été entendu en juin 2004 et rejeté sur le fond. La Cour a confirmé la conclusion de la Section de première instance selon laquelle M^{me} L'Écuyer avait consenti, du moins implicitement, à la communication en cause. Elle a conclu qu'il était inutile de traiter des autres aspects de l'appel portant sur les secteurs de compétence.

Commissaire à la protection de la vie privée du Canada c. Aéroports de Montréal

N^o de dossier de la Cour fédérale T-336-02

Plainte

L'employée d'un aéroport a déposé deux plaintes distinctes, affirmant que son employeur avait refusé d'acquiescer à plusieurs demandes d'accès à ses renseignements personnels. La direction de l'aéroport a justifié son refus d'accès en invoquant deux exceptions prévues

En ce qui concerne le coordonnateur des relations avec les employés, le Commissaire a établi que, compte tenu de la participation directe de cette personne aux demandes d'accès, il était approprié que l'employeur l'informe de sa décision de refuser d'acquiescer à la demande d'accès. On a donc établi que cette partie de la plainte était non fondée.

Au sujet de la communication aux représentants syndicaux, le Commissaire a la protection de la vie privée est d'avis que l'employeur avait été autorisé par consentement implicite à envoyer les copies de la réponse à ces parties seulement si la plaignante avait indiqué qu'elle leur avait fait parvenir des copies de ses demandes d'accès. Il a conclu qu'il n'y avait pas eu de consentement implicite en l'espèce et qu'une personne raisonnable aurait estimé que la communication des renseignements aux représentants syndicaux était inacceptable.

sans son consentement, communiqué ses renseignements personnels à des tierces parties. relations avec les employés de l'aéroport. Elle s'est donc plainte que son employeur avait, la lettre à trois autres personnes : deux représentants syndicaux et le coordonnateur des Ce dernier a refusé de donner suite à ses demandes dans une lettre et envoyé copie de Mme L'Écuyer a demandé d'avoir accès aux renseignements détenus par son employeur.

Plainte

Nos de dossier de la Cour fédérale T-2228-01 and A-259-03

Diane L'Écuyer c. Aéroports de Montréal et le Commissaire à la protection de la vie privée du Canada

La demande originale à la Section de première instance a été abandonnée en mars 2004, dans le cadre d'un règlement conclu entre M. Mahieu et IMS.

mais après l'audience de novembre 2003, la demande a fait l'objet d'un non-lieu.

qu'il verse une garantie pour les coûts. La Cour a ordonné à M. Mahieu de déposer une garantie financière de 12 000 \$ et a mentionné qu'elle avait des raisons de croire que M. Mahieu utilisait la Loi à des fins accessoires et inappropriées, compte tenu du fait que ses propres renseignements personnels n'étaient pas en jeu. Elle a accordé un appel de cette ordonnance à M. Mahieu en janvier 2003. La décision a été portée en appel par IMS,

Ronald G. Maheu c. IMS Health Canada et al.

Nos de dossier de la Cour fédérale T-1967-01 et A-31-03

Plainte

M. Maheu s'est plaint que IMS Health Canada avait communiqué de manière inappropriée des renseignements personnels en vendant des données sur les habitudes de prescription des médecins sans avoir obtenu leur consentement.

Le Commissaire a mis l'accent sur la question de savoir si les renseignements en cause étaient des renseignements personnels au sens et selon la portée et l'objet de la *LPRPDÉ* et conclu que le sens de « renseignements personnels » n'est pas assez vaste pour englober tous les renseignements associés à une personne. En se fondant sur cette interprétation, le Commissaire a conclu que des renseignements sur les ordonnances, qu'il s'agisse d'ordonnances individuelles ou d'habitudes de prescription, ne sont pas des renseignements personnels concernant un médecin. Il a plutôt présenté ces renseignements comme concernant un processus professionnel qui débouche sur la délivrance de l'ordonnance et a conclu qu'ils doivent donc être considérés comme un produit du travail.

Intervention du CPVP

Le Commissaire a présenté des arguments par écrit sur la première demande, qui ont porté uniquement sur le renvoi au Commissaire à la protection de la vie privée et ne s'est pas prononcé sur le résultat qu'il convient de tirer des faits.

Le Commissaire est également intervenu dans la procédure d'appel et a comparu pour aider la Cour à bien interpréter la *LPRPDÉ*. Il a expliqué qu'une personne peut déposer une plainte concernant les pratiques en matière d'information d'une organisation sans égard au fait que celle-ci recueille, utilise ou communique ou non des renseignements personnels concernant le plaignant.

État de la situation

M. Maheu a présenté une demande d'audition devant la Cour fédérale en novembre 2001.

IMS a présenté une requête demandant soit de rejeter la demande pour des motifs voulant que la demande ait été présentée à des fins inappropriées, soit de demander à M. Maheu

des frais des clients qui demandent la « non-publication » de leur numéro de téléphone. M. Englander soutient que les mesures prises par Telus sont contraires aux paragraphes 5(1) et (3) de la *Loi* ainsi qu'à plusieurs clauses de l'annexe 1 de la *Loi*.

Au sujet du consentement, le Commissaire a conclu que l'entreprise avait de fait obtenu un consentement valable de manière implicite et se conformait aux règlements concernant les renseignements mis à la disposition du public. Il a mis l'accent sur la question que l'entreprise posait à ses clients quant à la façon dont les renseignements les concernant devraient figurer dans les pages blanches et a établi que la question implicite en soi la publication éventuelle des renseignements dans des annuaires auxquels le public a accès. Puisque les renseignements publiés par la suite sur d'autres supports correspondent simplement à ceux qui sont publiés dans les pages blanches, ils sont également tenus pour des renseignements auxquels le public a accès et il est possible de les recueillir, de les utiliser et de les communiquer sans le consentement de la personne concernée.

Au sujet des frais exigés pour la non-publication des renseignements concernant les clients, le Commissaire a signalé l'Ordonnance Télécom 98-109 du CRTC qui stipule que les sociétés de télécommunications peuvent exiger jusqu'à 2 \$ par mois pour un service de numéro non publié. Par conséquent, il a conclu que l'entreprise en cause était habilitée à exiger son tarif mensuel de non-publication établi à 2 \$ et que cette mesure n'était pas déraisonnable.

Intervention du CPVP

Le Commissaire à la protection de la vie privée a obtenu l'autorisation d'intervenir dans cet appel sur les questions qui : (1) se rapportent aux conclusions du Commissaire à la protection de la vie privée et (2) à la compétence du CRTC de prendre des ordonnances en matière de vie privée qui ne limitent pas la compétence de la Cour fédérale aux termes de la *LPRPD*.

État de la situation

Il s'agit de la première demande de contrôle judiciaire déposée à la Cour fédérale aux termes de la *LPRPD*. La demande a fait l'objet d'un non-lieu en juin 2003 à la Cour fédérale.

M. Englander a déposé un appel devant la Cour d'appel fédérale le 28 août 2003. Aucune date d'audience n'a encore été fixée.

desquelles des mesures correctives ont été recommandées. Cet exercice, qui vise à savoir si les recommandations du Commissaire ont été adoptées, devrait être mené par voie de correspondance. Le Commissariat mènera d'autres enquêtes lorsqu'il sera saisi d'éléments de preuve de non-conformité.

DEVANT LES TRIBUNAUX

Aux termes de l'article 14 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), une personne ayant porté plainte a le droit, à l'issue de l'enquête du Commissaire et après le dépôt de son rapport, de déposer une demande d'audience à la Cour fédérale du Canada sur toute question traitée dans ce rapport. Ces questions doivent figurer parmi les clauses et les articles de la LPRPDE qui sont énumérés à l'article 14. Aux termes de cet article, le Commissaire peut, de sa propre initiative, déposer directement une demande à la Cour fédérale à l'égard d'une plainte.

Aux termes de l'article 15 de la *Loi*, le Commissaire est autorisé à déposer une demande de comparution à la Cour fédérale dans les circonstances décrites ci-après. Il peut, avec le consentement du plaignant, demander directement une audience à la Cour sur toute question visée par l'article 14, comparaitre devant la Cour au nom de tout plaignant qui a présenté une demande d'audience en vertu de l'article 14 ou, avec l'autorisation de la Cour, comparaitre comme partie à une instance engagée en vertu de l'article 14.

Entre le 1^{er} janvier 2001 et le 31 décembre 2003, 20 demandes ont été déposées devant la Cour fédérale au titre de la LPRPDE. La plupart d'entre elles ont été abandonnées, rejetées ou résolues avant que la Cour ne se soit prononcée. Les demandes en vertu de la LPRPDE qui suivent méritent qu'on s'y arrête.

Mathew Englander c. Telus Communications Inc. et le Commissaire à la protection de la vie privée du Canada

N^{os} de dossier de la Cour fédérale T-1717-01 et A-388-03

Plainte

M. Englander a soutenu que Telus utilise et communique les noms, adresses et numéros de téléphone de ses clients dans les pages blanches de son annuaire et aillieurs, à l'insu de ses clients et sans avoir obtenu leur consentement. En outre, Telus exige indûment

Nous avons également reçu des appels et des lettres de particuliers qui faisaient part de leur insatisfaction à l'égard d'organisations, alléguant qu'elles avaient mal géré leurs renseignements personnels, leur avaient refusé l'accès à leurs renseignements personnels, avaient refusé d'apporter les corrections demandées aux renseignements personnels ou n'avaient pas appliqué de mesures appropriées de sécurité pour protéger leurs renseignements personnels.

Statistiques relatives aux demandes de renseignements

(du 1^{er} janvier au 31 décembre 2003)

9 288	Demandes téléphoniques reçues
4 134	Demandes écrites reçues (lettre, courriel, télécopie)
13 422	Nombre total de demandes reçues

EXAMENS ET PRATIQUES EN MATIÈRE DE VIE PRIVÉE

Vérifications et examens de la conformité aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

Le mandat de la Direction des examens et des pratiques en matière de vie privée consistant à mener des vérifications d'organisations du secteur privé est prévu au paragraphe 18(1) de la LPRPDE. La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) autorise le Commissaire à vérifier la conformité des organisations du secteur privé avec la Loi s'il existe des motifs raisonnables de croire que celles-ci contreviennent à la Loi. Conformément à la LPRPDE, le Commissaire ne peut mener une telle vérification que s'il existe des « motifs raisonnables » de croire qu'une organisation contrevient à une disposition de la Loi.

À ce jour, le Commissariat n'a mené aucune vérification de la conformité avec la loi auprès d'une organisation du secteur privé en vertu du paragraphe 18(1) de la LPRPDE. Les éléments de preuve de la non-conformité avec la LPRPDE ont été portés à l'attention du Commissariat par l'entremise de plaintes et de demandes de renseignements. La plupart des cas de conformité qui nous ont été signalés traitaient d'incidents distincts qui se prétaient à un réglément dans le cadre des processus de plaintes et de demandes de renseignements.

Cela dit, au cours de la prochaine année, le Commissariat prévoit examiner les enquêtes achevées aux termes de la LPRPDE pour assurer le suivi des plaintes fondées à l'égard

Cet incident n'a suscité aucune plainte auprès du Commissariat de la part des personnes touchées.

Vente d'ordinateurs d'une banque contenant des renseignements personnels des clients

Les médias ont publié le cas d'un revendeur qui avait acheté deux ordinateurs d'une banque et les avaient mis en vente sur un site aux enchères en ligne avant de s'apercevoir qu'ils contenaient des renseignements personnels des clients de la banque. Il a par la suite communiqué avec la banque.

Ce qui est arrivé, c'est que, lorsque le revendeur est allé chercher les ordinateurs qu'il avait achetés, un employé de l'entreprise dont les services avaient été retenus pour effacer le contenu des ordinateurs et disposer du matériel informatique de la banque a, par inadvertance, pris les deux ordinateurs d'un lot de serveurs qui n'avaient pas encore été effacés.

La banque a identifié 350 clients dont les renseignements personnels étaient contenus sur l'un ou l'autre ordinateur. Une foule de renseignements personnels variés ont été trouvés. La banque a communiqué par téléphone avec les clients touchés et donné des entrevues aux médias pour confirmer que la situation était sous contrôle et que les comptes des clients étaient en sécurité. Elle a également mené une vérification de l'entrepreneur en cause et trouvé de nombreuses lacunes. Elle a revu le processus de disposition et rédigé une nouvelle ligne directrice sur le sujet.

Le Commissariat n'a reçu aucune plainte sur cet incident par les personnes touchées.

Demandes de renseignements

Le Commissariat a donné suite à des milliers de demandes de renseignements provenant du grand public et d'organisations qui voulaient obtenir des conseils et de l'aide concernant des enjeux en matière de vie privée dans le secteur privé.

Dans la plupart des cas, les appels et les articles de correspondance reçus au dernier semestre de 2003 concernant la LPRPD provenaient de grandes et de petites entreprises désireuses d'obtenir des directives afin de se préparer en vue de l'entrée en vigueur de la Loi le 1^{er} janvier 2004.

succursales, tous les bureaux et guichets ont des bacs qui sont vidés dans une déchiqueteuse confidentielle chaque jour.

La banque a communiqué par téléphone et par écrit avec tous les clients touchés pour les informer de l'enquête policière en cours. Elle a offert des conseils précis ainsi que des mesures de protection supplémentaires en fonction du niveau de risque de vol d'identité que chacune des situations présentait. Elle leur a également recommandé de surveiller leurs comptes pour déceler d'éventuelles activités suspectes, de signaler le courrier manquant et de bien protéger leurs dossiers financiers. La banque a transmis un rappel aux employés des succursales de la région visée concernant les politiques satisfaisantes d'élimination des ordures. La politique doit être revue mensuellement par les employés des succursales. De plus, les poubelles à l'intention des clients ont été enlevées et seuls des réceptacles encastres seront utilisés.

En ce qui concerne la troisième banque, 575 clients de la région ont été touchés. On a recouvert quatre rapports contenant le nom de multiples clients, représentant 438 des clients susmentionnés. Les renseignements personnels visant les autres clients ont été trouvés dans un éventail de documents se rapportant à des clients particuliers.

La banque estime que certains des documents ont été trouvés dans les ordures parce qu'ils étaient souillés ou déchirés à la main. D'autres documents étaient en bon état et la banque n'a pu affirmer avec certitude s'ils ont été trouvés dans les ordures ou si le suspect les a volés dans les bacs de déchiquetage à l'intérieur de la banque. Ces boîtes non verrouillées sont situées près des postes de travail des conseillers financiers et en activités commerciales.

Les clients visés ont été regroupés selon le risque (élevé, moyen ou faible) de vol d'identité et de fraude que présentait la communication des renseignements les concernant. Des représentants des succursales ont communiqué avec les clients par téléphone et leur ont dit quels renseignements précis avaient été communiqués. La banque a invité les clients des groupes à risque élevé et moyen à rencontrer un représentant de la banque pour revoir leurs comptes afin d'y déceler des activités suspectes et à ouvrir de nouveaux comptes. Elle leur a également conseillé de communiquer avec les bureaux de crédit ou DRHC si un document contenant leur NAS avait été trouvé afin d'atténuer les risques de fraudes. Elle a dit à tous ses clients de garder un œil sur leurs comptes.

La banque a passé en revue les procédures adéquates avec les gestionnaires des quatre succursales touchées. Elle a également confié à un groupe de travail l'examen des procédures et pratiques de la banque en matière de destruction des dossiers confidentiels et le soin de recommander les changements qui s'imposent.

Incidents visés par la LPRPDÉ

Le Commissariat a également mené 13 enquêtes sur des incidents. Les incidents sont des questions dont le Commissariat prend connaissance à partir de diverses sources, notamment les médias et les organisations qui les signalent d'eux-mêmes. Habituellement, dans pareil cas, la victime n'est pas nommée et le Commissariat n'a reçu aucune plainte.

Communications par l'entremise d'une benne à ordures

Le Commissariat a appris dans des reportages médiatiques que les services policiers avaient trouvé des dossiers financiers de clients de banques dans l'appartement d'un suspect. Cet homme prétendait avoir obtenu ces documents dans des bennes à ordures de succursales de trois banques.

Des représentants des trois banques ont récupéré les documents et les ont analysés dans le dessein d'en trouver l'origine, d'identifier les clients visés et de prendre les mesures correctives qui s'imposaient.

La première banque a identifié les renseignements personnels de 40 clients provenant de sept succursales. Elle a établi que les documents avaient vraisemblablement été trouvés dans les ordures. La banque avait déjà instauré une politique concernant la destruction des renseignements personnels mais les dispositions de cueillette des ordures varient d'une succursale à l'autre. Certaines succursales passent des contrats de déchiquetage avec des entreprises de l'extérieur tandis que d'autres exigent des employés qu'ils détruisent eux-mêmes les documents, soit en les déchiquetant, soit en les déchirant à la main.

La banque a vérifié les comptes et avisé par téléphone tous les clients touchés qu'aucune activité suspecte n'avait été décelée. Elle s'est engagée à continuer de surveiller l'activité des comptes et a demandé aux clients touchés de faire de même. La banque leur a également donné le choix de fermer leurs comptes actuels et d'en ouvrir de nouveaux. Elle a de nouveau émis sa politique et ses procédures en matière de disposition de renseignements personnels et informé les succursales qu'elles devaient de nouveau les présenter aux employés. Elle songe à appliquer un programme national de fournisseurs de bacs verrouillés et de destruction périodique des documents confidentiels.

Quant à la deuxième banque, elle a récupéré des renseignements personnels concernant 44 clients. Elle a conclu que les documents avaient été trouvés dans des poubelles internes et externes de même que dans des bacs internes de recyclage et de déchiquetage. Dans les

- de recueillir des renseignements médicaux des employés uniquement à des fins raisonnables;
- d'indiquer ces fins;
- d'obtenir un consentement valable;
- de limiter leurs pratiques de collecte, d'utilisation et de communication à ces seules fins.

En fin d'analyse, il incombe aux organisations de s'assurer :

sur la quantité de renseignements que l'employeur recueille, utilise et communique.

Il convient en outre de signaler que d'autres textes de loi, comme les lois sur le travail, sur les indemnités en cas d'accident du travail ou sur les droits de la personne peuvent influencer les politiques et procédures de traitement des renseignements personnels en leur possession.

Aux termes de la *LPDP*, les organisations sont tenues d'établir et de diffuser des De telles mesures, il va sans dire, supposent l'adoption de politiques et procédures claires.

Le Commissariat a établi en toute clarté que des mesures de sécurité rigoureuses doivent être instaurées pour traiter les renseignements médicaux des employés, surtout les renseignements diagnostiques. Plus précisément, les renseignements médicaux doivent être conservés à part du dossier personnel de l'employé, dans un endroit protégé. Les renseignements diagnostiques fournis ne doivent être traités que par des professionnels de la santé qualifiés et non par des spécialistes des ressources humaines. Il convient de fournir aux gestionnaires uniquement des renseignements restreints, comme la date prévue de retour au travail. Les superviseurs n'ont en général pas besoin de connaître en détail la maladie d'un employé.

Le Commissariat a établi en toute clarté que des mesures de sécurité rigoureuses doivent être instaurées pour traiter les renseignements médicaux des employés, surtout les renseignements diagnostiques. Plus précisément, les renseignements médicaux doivent être conservés à part du dossier personnel de l'employé, dans un endroit protégé. Les renseignements diagnostiques fournis ne doivent être traités que par des professionnels de la santé qualifiés et non par des spécialistes des ressources humaines. Il convient de fournir aux gestionnaires uniquement des renseignements restreints, comme la date prévue de retour au travail. Les superviseurs n'ont en général pas besoin de connaître en détail la maladie d'un employé.

sans attestation de médecin.

les cas d'absences suspectes ou lorsqu'un employé a épuisé ses crédits de congés de maladie

Toutefois, le Commissariat estime qu'il n'est pas raisonnable d'exiger un diagnostic dans d'un employé handicapé ainsi que pour établir si un employé a droit à des prestations.

l'aptitude au travail d'un employé et prendre des mesures d'adaptation à l'intention

Jusqu'à maintenant, nous reconnaissons qu'ils peuvent être nécessaires pour déterminer

peut avoir besoin de recueillir ces renseignements dans des circonstances très restreintes.

renseignements diagnostiques ont été exigés, le Commissariat a reconnu que l'employeur

année a été l'exigence de fournir un diagnostic. Dans les affaires pour lesquelles des

De loin, la question la plus litigieuse soulevée par les employés au cours de la dernière

L'entreprise a mis en place des procédures et des politiques qui permettent de protéger les renseignements médicaux personnels d'un employé. Plus particulièrement, les renseignements médicaux sont classés à part du dossier personnel, puis stockés dans des zones d'archivage sécuritaires. Les renseignements médicaux informatisés sont également protégés.

Mesures prises par le CPVP

Nous avons établi que, compte tenu de la responsabilité de l'entreprise de verser le salaire du plaignant pendant les six premiers mois de son absence et de ses obligations conformément aux lois et règlements canadiens sur les droits de la personne de prendre des mesures d'adaptation à l'intention des employés handicapés, les motifs de la collecte des diagnostics étaient légitimes et appropriés.

Lorsque nous nous sommes penchés sur la manière dont l'entreprise a réussi à limiter la collecte de renseignements personnels, nous avons constaté que les lignes directrices de la Commission canadienne des droits de la personne précisent qu'un employeur a le droit, aux termes de la *Loi canadienne sur les droits de la personne*, de demander assez de renseignements pour être en mesure de déterminer s'il est tenu de prendre des mesures d'adaptation concernant une personne handicapée, ce qui peut exiger la consultation d'un médecin spécialiste. Nous sommes d'avis que les documents médicaux que l'employeur voulait obtenir étaient manifestement liés aux obligations de l'entreprise de prendre des mesures d'adaptation à l'intention du plaignant et n'étaient pas excessifs.

Nous sommes également convaincus que l'entreprise avait déjà des politiques et des procédures en place qui décrivaient les motifs de la collecte de renseignements de santé, comment ils étaient traités et par qui, ainsi que les rôles respectifs de l'employeur, de l'employé et du service de santé. Ces renseignements ont été mis à la disposition de tous les employés sur différents supports, ce qui satisfait aux obligations de l'entreprise en vertu de la *LRPDE* de ne pas recueillir des renseignements personnels de façon arbitraire et de préciser le genre de renseignements recueillis dans le cadre de ses politiques et pratiques de traitement des renseignements.

Nous avons donc conclu que la plainte était non fondée.

Sommaire de la position du Commissariat à ce jour en matière de renseignements médicaux des employés

Les employeurs recueillent des renseignements médicaux sur les employés pour nombre de raisons, lesquelles doivent être appropriées et légitimes dans les circonstances et clairement indiquées. Les renseignements recueillis doivent être limités à ces fins.

médecin a fourni, au total, trois rapports similaires, tous indiquant que le pronostic était

inconnu.

Par la suite, le médecin a dit au plaignant qu'il pouvait retourner au travail à temps partiel. Le médecin a appuyé la demande du plaignant voulant que celui-ci soit muté à un milieu de travail différent, qui comprendrait d'avantage de fonctions opérationnelles que de fonctions administratives. Puisque l'entreprise n'avait pas reçu de demande du plaignant à cet effet, l'infirmerie des services de santé au travail a demandé des renseignements supplémentaires au médecin sur les troubles de santé du plaignant. Elle a également demandé des renseignements sur la capacité du plaignant d'effectuer un travail physique, à la lumière d'une blessure qu'il s'était faite quelques années auparavant et qui avait causé sa mutation vers un poste plus administratif.

Par la suite, le plaignant a présenté une demande officielle de mutation pour des raisons de santé. L'entreprise a demandé de plus amples renseignements médicaux et indiqué qu'une évaluation médicale indépendante serait peut-être nécessaire. L'entreprise ayant refusé la demande du plaignant, le médecin de ce dernier a de nouveau écrit une lettre à l'employeur appuyant la demande du plaignant. L'entreprise a répondu en affirmant qu'elle devait rencontrer un spécialiste avant de répondre à cette requête. Le plaignant et un représentant de son syndicat se sont opposés et ont prétendu que l'entreprise devait accepter les évaluations médicales du plaignant. Le plaignant a fini par retourner à son poste administratif.

L'entreprise avait instauré une politique sur les congés de maladie prolongés conformément à laquelle l'employé doit signer un formulaire de consentement autorisant son médecin à communiquer des renseignements médicaux liés à la maladie de l'employé aux professionnels en santé au travail de l'entreprise et à discuter de ce sujet directement avec eux. Le formulaire précise les motifs de l'entreprise pour recueillir de tels renseignements, à savoir un examen pour déterminer l'admissibilité aux prestations et l'aptitude à l'emploi. Le formulaire comprend des questions sur les problèmes de santé, les soins et le pronostic médicaux de l'employé, ce qui comprend le diagnostic.

Les membres du personnel en santé au travail de l'entreprise ont été les seuls à prendre connaissance de ces renseignements. Ils sont tenus par leur code de déontologie respectif d'assurer la confidentialité. Ils ont fourni aux gestionnaires seulement l'information concernant l'aptitude à travailler et les limites physiques de l'employé. Des renseignements détaillés concernant la politique de l'entreprise sont accessibles à tous les employés sur le site Intranet de l'entreprise et dans une brochure.

provinciale en vigueur qui régit l'indemnisation des travailleurs à laquelle elle est assujettie. Aux termes de la législation, les cotisants sont tenus d'aviser immédiatement la CAT de toute incapacité liée au travail ou allégation d'incapacité. La législation donne aussi à la CAT le pouvoir d'enquêter sur les demandes et les cotisants sont obligés d'y répondre.

Mesures prises par le CPVP

Nous avons déterminé que les motifs de collecte de renseignements diagnostiques de l'entreprise, à savoir gérer le régime d'invalidité des employés, étaient raisonnables et légitimes. Nous avons déterminé également que ces motifs avaient été identifiés pertinemment, que les renseignements personnels recueillis étaient tous nécessaires à la réalisation des motifs invoqués et que la plaignante avait dûment consenti à la collecte de ceux-ci.

Quant à la plainte concernant la communication, qui a manifestement été faite à l'insu de la plaignante et sans son consentement, nous avons établi que la communication en question était requise par la loi et, par conséquent, permise en vertu d'un alinéa de la LPRPDE qui prévoit les communications à l'insu de l'intéressé et sans son consentement si elles sont exigées par la loi.

Nous avons conclu que les plaintes étaient non fondées. Néanmoins, l'enquête a démontré que l'entreprise n'avait pas prévu de politiques, procédures, lignes directrices ou documents de formation à l'intention du personnel portant précisément sur l'information concernant les employés. Par conséquent, nous avons recommandé à l'entreprise d'instruire des politiques et pratiques se rapportant précisément au traitement des renseignements personnels des employés, conformément aux principes d'imputabilité énoncés dans la LPRPDE.

Le Commissariat assure actuellement le suivi auprès de l'organisation pour s'assurer que les recommandations ont été mises en œuvre.

Diagnostic : raisonnable dans les circonstances

Aperçu

Un employé qui voulait être muté à un autre poste pour des raisons de santé estimait que son employeur essayait de recueillir plus de renseignements personnels à son sujet qu'il n'était nécessaire. Pendant qu'il était en congé, son employeur lui a demandé d'autoriser son médecin à remplir un formulaire indiquant son pronostic, ses restrictions, ses traitements médicaux et ses aptitudes. Le médecin a posé un diagnostic et donné des renseignements sur le traitement, mais n'a pas rempli les sections concernant les restrictions et les aptitudes. Le

du médecin traitant. Bien qu'elle ait fourni les renseignements, elle a trouvé à redire sur le fait qu'un médecin praticien soit obligé de poser un diagnostic précis. Elle soutenait que l'employeuse devrait se contenter d'une description plus générale sur la nature de son incapacité, soit une « maladie », une « blessure » ou une « incapacité liée au travail ».

À sa grande surprise, quelques mois après avoir présenté le formulaire, la plaignante a reçu une lettre de la Commission des accidents du travail (CAT) provinciale l'informant qu'elle rejetait sa demande d'indemnisation par manque de preuve. La Commission a établi que son incapacité n'était pas liée au travail. La lettre faisait référence à un renseignement que l'arbitre de la CAT avait reçu de l'employeuse de la plaignante. Cette dernière n'avait pas présenté de demande d'indemnisation à la CAT et estimait que le renseignement fourni par son employeuse ne se rapportait pas à son incapacité. Elle estimait donc que les communications faites par son employeuse, à son insu et sans son consentement, n'étaient ni appropriées ni justifiées.

L'enquête a établi que l'employeuse avait avisé la Commission d'une présumée incapacité de travailler liée à l'emploi et présenté une demande d'indemnisation au nom de l'intéressée. L'arbitre de la CAT a obtenu une copie de l'original du formulaire de demande de renseignements d'ordre médical de la plaignante et posé des questions à l'employeuse au sujet de l'incapacité en cause. La représentante de l'employeuse, une coordonnatrice des ressources humaines, a confirmé que la plaignante s'était absentée auparavant pour une raison similaire, mais qu'à son avis, cette absence était attribuable à des raisons personnelles, sans lien avec le travail. Cependant, elle ne pouvait pas dire si l'absence en cause actuellement était liée au travail.

En ce qui a trait à la collecte de renseignements médicaux, l'entreprise a allégué qu'elle devait obtenir des diagnostics précis afin de gérer le régime d'assurance-salaire en cas d'invalidité de courte ou de longue durée des employés. Notamment, l'admissibilité aux avantages dans le cadre du régime à long terme est établie en fonction des avantages à court terme obtenus pendant un certain nombre de jours pour une incapacité déterminée.

L'employeuse a fait savoir que les objectifs de la collecte des renseignements sont indiqués dans sa politique régissant le régime d'assurance-salaire en cas d'invalidité de courte durée et dans le formulaire de demande de renseignements d'ordre médical. Elle a soutenu que la collecte visait uniquement les fins indiquées. Par ailleurs, elle a signalé que le consentement des employés était obtenu puisque le formulaire de demande de renseignements d'ordre médical signé par les employés contient un énoncé relatif au consentement.

En ce qui concerne la communication à la CAT, l'entreprise a souligné que la communication était non seulement appropriée mais qu'elle était exigée par la législation

employés dépassaient la limite permise pour un congé de maladie sans attestation de médecin, un certificat sans diagnostic aurait été suffisant. Comme l'employeur a fini par le reconnaître, il n'est pas nécessaire d'exiger des employés qu'ils fournissent des renseignements diagnostiques dans le cas d'absences suspectes.

À notre avis, l'entreprise n'a pas démontré de manière satisfaisante qu'elle devait poser des questions sur la nature de la maladie des plaignants afin de s'assurer qu'ils étaient aptes à reprendre leurs fonctions normales ou de prendre des dispositions pour leur retour au travail.

En fait, dans les circonstances entourant ces affaires, à savoir lorsque les absences des employés dépassaient la limite permise pour un congé de maladie sans attestation de médecin ou que leurs absences étaient suspectes, nous avons conclu qu'il était à la fois inutile et inapproprié que l'organisation exige ces renseignements. Nous avons donc conclu que les plaintes étaient fondées.

Nous avons recommandé à l'entreprise de retirer l'exigence selon laquelle les employés désignés à risque ont l'obligation d'inclure un diagnostic dans le certificat médical qu'ils présentent et de limiter désormais la collecte de renseignements diagnostiques aux cas d'employés où cela est clairement nécessaire pour réaliser les fins légitimes. Nous lui avons également recommandé de modifier en conséquence sa politique sur les congés de maladie.

Enfin, nous avons recommandé à l'entreprise de revoir sa décision de refuser un congé de maladie aux employés ayant dépassé la limite permise pour un congé de maladie sans attestation de médecin et refusé de remettre un diagnostic médical.

Le Commissariat assure actuellement le suivi auprès de l'organisation pour s'assurer que les recommandations ont été mises en œuvre.

Diagnostic : objectifs raisonnables

Aperçu

La nécessité d'obtenir des renseignements diagnostiques et les éventuels destinataires des renseignements médicaux communiqués ont été le sujet de plaintes formulées par une personne à l'égard de son ancienne employeuse.

Au début de son congé de maladie prolongé, la plaignante a présenté à l'employeuse un formulaire de demande de renseignements d'ordre médical où figurait le diagnostic précis

Diagnostic : surabondance de renseignements

Aperçu

Plusieurs employés se sont plaints que leur employeur avait exigé qu'un diagnostic médical figure sur les certificats de congé de maladie. Ces employés avaient épuisé le nombre de jours de congé de maladie sans certificat qui leur était permis chaque année ou montraient ce que leur employeur a estimé être un comportement suspect au titre des congés.

Les plaignants ne s'opposaient pas à ce que l'employeur leur demande s'ils avaient vu un médecin et si des restrictions leur avaient été imposées, y compris tout médicament qu'ils pourraient prendre, les empêchant de s'acquitter de leurs fonctions en toute sécurité. Ils s'opposaient toutefois au fait que leur employeur les oblige à fournir un *diagnostic médical* pour justifier les congés de maladie.

L'entreprise a expliqué que deux motifs justifiaient une demande de diagnostic. Le premier avait trait aux employés « à risque » qui travaillaient souvent de longues heures seuls et s'acquittaient de tâches de nature critique pour la sécurité et qui sont exigeantes sur le plan physique. L'entreprise a soutenu que le médecin d'un employé ne connaît pas la nature exacte de son travail, mais qu'un agent de santé et sécurité au travail de l'entreprise est plus en mesure de juger s'il est sécuritaire qu'un employé retourne à ses fonctions habituelles. L'entreprise n'a cependant pas prouvé qu'elle utilisait à cette fin de façon habituelle les renseignements diagnostiques. De fait, dans un cas, elle a même autorisé le retour au travail d'un employé « à risque » même si son médecin ne lui avait pas communiqué de diagnostic.

La deuxième raison pour laquelle l'employeur exige un diagnostic médical se rapportait aux « absences suspectes », c'est-à-dire celles qui surviennent immédiatement avant ou après des vacances ou durant une période pour laquelle l'entreprise avait antérieurement refusé d'accorder des congés. L'entreprise se réservait le droit d'exiger un certificat médical, y compris un diagnostic, si elle jugeait l'absence suspecte.

Après des discussions avec le Commissariat, l'organisation a convenu qu'elle ne demanderait plus aux employés de présenter un certificat médical avec diagnostic dans le cas d'absences suspectes et qu'elle reverrait l'obligation qu'ont les employés « à risque » de présenter un diagnostic médical.

Mesures prises par le CPVP

Dans nos conclusions, nous avons indiqué que, même s'il était tout à fait approprié et raisonnable pour l'employeur d'exiger un certificat médical lorsque les absences des

La Loi sur la protection des renseignements personnels et les documents électroniques s'applique aux renseignements personnels, incluant des renseignements sur la santé, des renseignements sur des employés dans des ouvrages, des installations, des entreprises et des secteurs d'activités fédéraux. En 2003, le Commissaire a reçu de nombreuses plaintes de fonctionnaires qui alléguaient que leurs employeurs recueillaient trop de renseignements médicaux ou les communiquaient de manière indue. Quelques affaires dignes de mention sont résumées ci-après et suivies d'un aperçu de la position du Commissariat à ce jour.

RENSEIGNEMENTS MÉDICAUX DES EMPLOYÉS

Mesures prises par le CPVP

Dans le cas de cette plainte fondée, nous avons conclu que les renseignements emmagasinés par les témoins temporaires et permanents constituaient des renseignements personnels aux fins de la LPPDE. Même si l'entreprise n'avait pas sciemment interdit l'accès à son site Web aux particuliers qui refusent de consentir à la collecte de renseignements personnels en désactivant les témoins permanents et qu'elle avait pris des mesures pour remédier à la situation, elle n'en avait pas moins refusé au plaignant l'accès à son site. Nous avons également signalé qu'elle n'avait pas rempli les conditions relatives à la connaissance et au consentement conformément à la LPPDE en ce qui concerne l'utilisation des témoins. Le Commissariat s'est réjoui du fait que l'entreprise ait accepté de publier une politique exhaustive sur son site Web concernant les témoins.

ayant désactivé les témoins permanents puissent utiliser le site.

L'organisation a également reconnu qu'elle n'avait ni inclus dans sa politique sur la protection de la vie privée ni sur son site Web de l'information sur les témoins. Elle a toutefois indiqué qu'elle est en train de produire une politique exhaustive sur l'utilisation des témoins, politique qui sera publiée dans un avenir prochain.

un éventail de renseignements. Les témoins permanents s'insèrent pour une période indéterminée sur le disque dur d'un usager sauf si l'usager les enlève manuellement son fureteur après avoir quitté le site Web. Les fureteurs Web permettent généralement aux usagers de désactiver les témoins en permanence ou temporairement. Le plaignant, qui avait désactivé les témoins permanents sur son fureteur, n'a pas pu se rendre à la page d'accueil parce que le site Web est codé de manière à lui refuser l'accès tant que le témoin n'a pas été emmagasiné sur son disque dur. L'organisation a reconnu que cet état de fait était attribuable à un problème d'application et a pris des mesures pour que les visiteurs

La collecte du NAS par le secteur privé est permise dans les situations suivantes :

- Les employeurs sont autorisés à recueillir le NAS de leurs employés afin de pouvoir leur remettre des relevés d'emploi et des feuillets T-4 aux fins de l'impôt sur le revenu.
- Les organisations, comme les banques, les coopératives de crédit, les courtiers et les sociétés de fiducie, sont tenues par la *Loi de l'impôt sur le revenu* de demander le NAS de leurs clients aux fins de leur déclaration d'impôts (p. ex., les comptes portant intérêt, les REER).
- Aucune organisation du secteur privé n'est légalement autorisée à demander le NAS de ses clients à des fins autres que celles liées au revenu. Si le compte d'un client ne porte pas intérêt (p. ex., un compte de crédit par opposition à un compte d'épargne), une institution financière n'est pas tenue par la loi de recueillir son NAS et le client n'est pas tenu de le fournir.
- Il n'existe aucune loi qui interdit à une organisation de *demande* le NAS d'un client ou à un client de fournir son NAS à des fins autres que celles liées au revenu.

Même s'il n'existe aucune loi qui interdit à une organisation de demander le NAS à des fins autres, comme l'identification, les organisations assujetties à la *LPDP* doivent indiquer clairement aux clients que la fourniture du NAS est facultative et n'est pas une condition d'obtention de service.

UTILISATION DES OUTILS DE SURVEILLANCE SUR LE WEB

Le « témoin » trébuche

Aperçu

Un particulier n'était pas satisfait de la configuration du site Web d'une organisation. Il nous a fait savoir qu'il n'avait pu avoir accès au site parce que son navigateur était configuré de manière à désactiver les « témoins » (communément appelés cookies). Il a de plus prétendu que l'organisation réunissait des renseignements personnels sur les visiteurs de son site Web à leur insu et sans leur consentement en omettant de leur faire savoir qu'elle plaçait un témoin sur le disque dur de leur ordinateur.

L'organisation en question a des témoins permanents et temporaires sur son site Web. Les « témoins » sont des petits fichiers texte qui peuvent recueillir et emmagasiner tout

La banque a déclaré que cette exigence de fournir un NAS à cette fin est facultative et qu'un client peut s'abstenir de le fournir ou demander à la banque de le retirer de son dossier.

Les versions électroniques et papier des formulaires de demande incluent une déclaration concernant l'utilisation du NAS aux fins d'identification. Cependant, ni l'une ni l'autre des versions n'indique que la communication du NAS est facultative. En fait, les deux types de formulaires contiennent des instructions stipulant qu'il est nécessaire de donner tous les renseignements demandés et précisent qu'en signant le formulaire ou en cliquant sur la boîte appropriée, le demandeur accepte toutes les conditions contenues dans le formulaire.

Mesures prises par le CPVP

Étant donné que la banque ne faisait pas un effort raisonnable pour s'assurer que le client soit adéquatement informé du caractère facultatif de la fourniture du NAS, nous avons conclu que la banque n'obtenait pas de consentement valable et explicite des demandeurs.

La banque a convenu que le libellé de ses formulaires de demande était problématique et a déclaré son intention d'apporter des changements aux formulaires en clarifiant le fait que la communication du NAS aux fins de correspondance des antécédents de crédit était facultative. Même si nous avons été satisfaits de la mesure prise par la banque, nous avons réitéré que le NAS n'est pas une pièce d'identité et ne doit pas être utilisé en tant que tel.

Utilisation du NAS dans le secteur privé

Cette plainte est caractéristique des nombreuses plaintes que le Commissariat a reçues en 2003 concernant l'utilisation du NAS à des fins d'identification par des organisations du secteur privé.

Les usages du NAS autorisés par la loi se sont accrus depuis sa création en 1964 et il est maintenant utilisé comme un numéro de compte-client dans l'administration du Régime de pensions du Canada et divers programmes d'assurance-emploi. Le gouvernement fédéral, dans un effort visant à prévenir l'usage du NAS comme un identificateur universel, a publié une politique limitant la collecte et l'usage du NAS à des lois, à des règlements et à des programmes particuliers.

concernant de telles violations de la vie privée devraient refléter le strict respect d'une organisation à l'égard de l'intégrité des renseignements personnels dont elle est responsable et, idéalement, la dissuader de commettre d'autres violations du même genre.

Nous avons formulé les recommandations suivantes :

- L'agence devrait songer à imposer et voir à ce que soient appliquées des sanctions plus sévères aux organisations clientes qui contreviennent aux dispositions contractuelles sur l'accès aux renseignements personnels des consommateurs. Les pénalités pourraient commencer par une suspension des services suivie d'une période de sursis, incluant des vérifications fréquentes et rigoureuses.

- L'agence devrait élaborer et suivre rigoureusement une politique qui stipulerait le moment et la façon d'aviser le plaignant des résultats d'une enquête interne sur une plainte.

Le Commissariat assure actuellement le suivi auprès de l'organisation pour s'assurer que les recommandations ont été mises en œuvre.

UTILISATION DES NUMÉROS D'ASSURANCE SOCIALE

Utiliser ou non le NAS

Apéryn

Une cliente s'est opposée à ce qu'une banque se serve des numéros d'assurance sociale (NAS) pour confirmer l'identité de demandeurs de cartes de crédit auprès des bureaux de crédit. La plaignante estime que la banque opérerait sans en avoir dûment informé les demandeurs et sans avoir obtenu leur consentement. Par ailleurs, elle était d'avis que le libellé du contrat de carte de crédit ne montre pas clairement aux clients qu'ils ont le choix de ne pas fournir leur NAS. Elle prétend que le libellé laisse plutôt l'impression que les demandeurs qui ne fournissent pas leur NAS n'obtiendront pas de carte.

La banque a soutenu que l'objectif visé par l'utilisation du NAS, qui consiste à jumeler fidèlement la demande au dossier des antécédents de crédit des créanciers, était légitime.

solvabilité non autorisées avaient été retirées de leurs dossiers parce que le client n'avait pas pu prouver qu'il y avait soit fin légitime, soit consentement valide. L'agence a présenté des excuses aux plaignants pour tous les désagréments subis.

En ce qui concerne le consentement, nous avons établi que l'agence avait communiqué des renseignements personnels concernant le couple sans leur consentement. Nous devions trancher la question de savoir si l'agence pouvait raisonnablement être tenue responsable en les circonstances.

Il est évident que l'agence ne savait pas que la demande avait été faite à l'insu et sans le consentement des plaignants mais, en fait, elle a présumé, en se fondant sur l'entente contractuelle, que le motif de l'entreprise était acceptable et que le consentement avait été obtenu en bonne et due forme. Par conséquent, à notre avis, l'agence a fait la communication de bonne foi et en présumant raisonnablement que le consentement avait été obtenu, étant donné les obligations énoncées dans l'entente et, par conséquent, n'a pas en soi enfreint la Loi.

Nous nous sommes montrés plus critiques de l'enquête menée par l'agence et du suivi qu'elle a donné à son enquête. Aux termes de la Loi, une organisation doit faire enquête sur toutes les plaintes qu'elle reçoit et prendre des mesures *appropriées* si l'enquête conclut que la plainte est fondée. L'agence a conclu que la plainte était fondée et a fini par prendre certaines mesures contre son client, mais ces dernières, surtout celle qui consiste à placer le client « en sursis », sont loin d'être appropriées pour les raisons suivantes :

- En premier lieu, les éléments de preuve indiquaient manifestement que les mesures avaient été prises seulement à la demande du Commissariat.
- Deuxièmement, il est raisonnable de penser qu'à la conclusion d'une enquête, l'organisation informe immédiatement le plaignant des résultats. Cependant, il semble que l'agence ait avisé les plaignants des résultats seulement après que le Commissariat lui ait suggéré de le faire.
- Troisièmement, et surtout, les mesures prises par l'agence n'étaient pas

appropriées étant donné la gravité de l'infraction. Bien que l'entente contractuelle type de l'agence conseille de « suspendre » ou d'« annuler » les services offerts aux clients lorsqu'il est légitime de croire qu'ils ont commis une violation, l'agence n'a imposé qu'une période de « sursis ». Nous ne pensons pas qu'une telle sanction soit suffisante pour que l'entreprise comprenne que sa conduite était inacceptable. Nous constatons que les mesures dissuasives

de crédit à la demande de la société mère, soit l'ancien employeur de l'épouse et avec qui celle-ci est en conflit.

Le couple a porté plainte à l'Agence qui a assuré les plaignants que leurs allégations feraient l'objet d'une enquête et qu'ils seraient tenus informés des résultats de cette enquête. Toutefois, trois semaines plus tard, lorsqu'ils ont téléphoné pour obtenir un compte rendu de la situation, un autre représentant de l'Agence leur a expliqué qu'aucune enquête interne n'avait été entreprise.

Le représentant a suggéré au couple d'effectuer ses propres recherches puisque la société mère en cause n'était pas un client de l'Agence et que, par conséquent, celle-ci n'était pas autorisée à faire enquête. Par la suite, un troisième représentant leur a assuré que l'Agence ferait enquête, mais cette fois-ci, les plaignants, incapables de faire confiance à l'Agence, ont porté plainte au Commissariat.

Mesures prises par le CPVP

Notre enquête a confirmé que le troisième représentant de l'Agence avait effectivement entrepris une enquête interne. Le propriétaire de la société mère a admis à l'Agence qu'il avait obtenu les renseignements de solvabilité personnels des plaignants, sans leur consentement, par l'intermédiaire du distributeur de crédit, qui est une succursale de son entreprise. Il a reconnu avoir enfreint les règlements concernant le crédit et expliqué que les circonstances exceptionnelles entourant le litige qui oppose son entreprise à l'ancienne employée, en l'occurrence son ex-femme, l'ont obligé à prendre de telles mesures.

L'entente contractuelle type qui existe entre le distributeur de crédit et l'Agence stipule que le client doit demander les rapports de solvabilité d'un consommateur seulement à des fins admissibles, et qu'il doit d'abord obtenir tous les consentements obligatoires du consommateur aux termes de la législation provinciale sur les enquêtes de solvabilité. L'entente stipule également que l'Agence peut mettre fin au service sur-le-champ si elle a raison de croire que le client a dérogé à une condition.

L'Agence n'a pas suspendu le service offert par le distributeur de crédit coupable de l'infraction, mais lui a plutôt imposé une année de sursis. L'Agence a affirmé au Commissariat que cette mesure dissuasive s'accompagnerait de vérifications et du contrôle des demandes de renseignements de solvabilité et qu'un autre manque à s'y conformer entraînerait la résiliation du contrat.

Une fois l'enquête terminée, l'Agence a attendu huit semaines avant d'aviser les plaignants des résultats. Elle a informé les plaignants que les demandes de renseignements de

Bien prendre la mesure

Aperçu

Deux employés d'une entreprise ont protesté lorsque leur employeur a décidé de se servir de données statistiques sur le travail pour mesurer leur rendement individuel. L'entreprise recueillait depuis longtemps les renseignements en question — volume, durée et type d'appels reçus par les téléphonistes — pour mesurer et gérer la charge de travail des bureaux. Toutefois, lorsque l'entreprise a commencé à se servir de ces données pour gérer le rendement, les plaignants, des téléphonistes, ont prétendu qu'elle recueillait et utilisait des données statistiques les concernant sans leur consentement.

Nous avons appris que l'entreprise avait avisé le personnel du changement de la politique au moyen d'exposés de groupe, par courrier électronique et à l'occasion de rencontres d'équipe et d'entrevues individuelles. La collecte et l'utilisation de statistiques sont également abordées dans la brochure sur la confidentialité destinée aux employés.

Chaque mois, les téléphonistes reçoivent un rapport dans lequel figurent leurs statistiques individuelles comparées aux objectifs prédéterminés concernant la durée des appels ou les attentes de l'entreprise. Ils peuvent également recevoir un rapport comprenant leurs statistiques par période de travail.

Mesures prises par le CPVP

Nous avons constaté que les objectifs de l'entreprise, à savoir surveiller et évaluer le rendement au travail de ses employés, étaient appropriés et que l'entreprise avait pris les mesures nécessaires pour informer ses employés de ces objectifs. Pour ce qui est de savoir si un employeur est tenu d'obtenir le consentement explicite d'un employé pour recueillir et utiliser de l'information aux fins de la gestion du rendement, nous avons établi que, lorsqu'une personne accepte de travailler pour une entreprise, elle consent explicitement aux conditions d'emploi. Les évaluations du rendement représentent l'une de ces conditions et les plaignants y ont consenti explicitement lorsqu'ils ont commencé à travailler auprès de l'entreprise. Nous avons conclu que la plainte était non fondée.

Vérification du rapport de solvabilité

Aperçu

Lorsque les membres d'un couple ont vérifié leurs rapports de solvabilité respectifs, ils ont constaté que l'agence d'évaluation du crédit avait communiqué des renseignements de solvabilité à un distributeur de crédit avec lequel ils n'avaient jamais traité directement. Le couple soupçonnait le distributeur de crédit en cause d'avoir eu accès à leurs dossiers

OBTENIR LE CONSENTEMENT

L'ex-femme, son avocat, la fille et l'agent de recouvrement

Abperçu

Une personne s'est plainte qu'une banque, par l'entremise d'une agence de recouvrement, a informé les membres de sa famille et l'avocat de son ex-femme de ses difficultés financières. Il est ressorti de notre enquête que l'agent de recouvrement s'occupant de son dossier a communiqué avec la fille du plaignant, son ancienne épouse et l'avocat de celle-ci. De fait, nombre de communications téléphoniques ont été échangées entre l'agent et ces personnes. Certains des appels ont été faits par l'agent, d'autres, par ces différentes personnes. Tous les appels reçus à l'agence et ceux faits à partir de l'agence, de même que les listes des appels, ont été consignés dans le système de suivi électronique de l'agence. Les renseignements contenus dans ce système peuvent être modifiés uniquement au cours de la période de deux heures suivant leur inscription initiale.

Mesures prises par le CPVP

Nous n'avons pu recueillir aucune preuve indiquant que l'agent a communiqué à ces personnes des renseignements particuliers sur la situation financière du plaignant ou profité des menaces de saisie de la propriété du plaignant, comme ce dernier le prétend. La banque effectue des vérifications auprès de l'agence afin de s'assurer que ses pratiques de protection des renseignements personnels sont conformes aux siennes. L'agent en question, un employé de longue date de la compagnie, a signé diverses déclarations de confidentialité et de déontologie avec l'agence.

Dans nos conclusions, nous avons remarqué que, même si la *LPRPDH* autorise une organisation à communiquer des renseignements personnels sans le consentement de l'intéressé et à son insu aux fins du recouvrement d'un montant dû, celle-ci ne lui donne pas *carte blanche* pour communiquer tous les renseignements qu'elle désire afin de recouvrer une dette.

En l'espèce, nous avons établi que les renseignements fournis à l'ex-épouse se limitaient à une référence à une dette en souffrance. L'avocat de celle-ci a refusé de fournir une confirmation écrite de ce que l'agent lui avait communiqué. Les témoignages de la fille et de l'agent se contredisaient, et il y n'existait aucune preuve documentaire indiquant qu'il y avait eu communication excessive de renseignements personnels sur le plaignant. Compte tenu de la situation, nous avons conclu que la plainte était non fondée étant donné que les actes de l'agent étaient conformes à l'exception à l'exigence de consentement afin de recouvrer une dette.

Le Commissariat assure actuellement le suivi auprès de l'organisation pour s'assurer que les recommandations ont été mises en œuvre.

UTILISATION NON AUTORISÉE DE RENSEIGNEMENTS PERSONNELS

La chartre avant les bœufs

Aperçu

Le Commissariat a appris que la directrice d'une succursale bancaire avait demandé à ses employés d'effectuer des vérifications du crédit des clients d'une banque, à leur insu et sans leur consentement, afin de prédéterminer lesquels seraient admissibles à une autorisation de découvert. Ils prévenaient ensuite les clients que le service avait été préautorisé et, s'ils l'acceptaient, on leur demanderait de signer une autorisation de vérification de la solvabilité, déjà effectuée.

Avant que nous prenions connaissance de cette pratique, la banque avait déjà entamé des mesures correctives. Lors d'une vérification de routine effectuée par la banque afin d'assurer la conformité à ses politiques, on a constaté qu'il y avait eu un manquement à la politique de la part de la succursale. La politique écrite de la banque stipule que les employés doivent obtenir le consentement du client avant de procéder à une vérification du crédit lorsque celui-ci présente une demande d'autorisation de découvert. La directrice de la succursale en a été informée et a immédiatement rectifié la situation.

La banque a convenu que la directrice avait mal interprété la formulation du consentement pour les comptes et cru par erreur que le consentement relatif à la mise à jour du crédit pouvait justifier une présélection en vue du service d'autorisation de découvert.

Résultat

Puisqu'il est indéniable que la directrice de la succursale en question a autorisé la collecte et l'utilisation des renseignements personnels des clients à leur insu et sans leur consentement, nous avons conclu que la banque avait contrevenu à l'exigence relative au consentement prévue à la LPRPDÉ. Toutefois, comme la banque a instauré une politique satisfaisante et décélé et corrigé le manquement à la politique avant même que le Commissariat ne soit saisi de l'affaire, nous avons conclu que la plainte était résolue.

présuné que la plaignante comprenait que les renseignements allaient servir à rechercher ses bagages, nous estimons qu'elle aurait au moins dû l'informer de la manière dont les renseignements seraient inscrits et dont les recherches s'effectueraient, à savoir au moyen d'un système mondial de recherche.

Faisant remarquer que, pour consentir à quelque chose, une personne doit d'abord en être informée, nous avons indiqué qu'il aurait d'abord fallu que le transporteur arien informe la plaignante des fins spécifiques de la collecte de renseignements personnels. Le transporteur ayant omis de le faire, il n'avait pas de raison valable pour conclure qu'elle y consentait.

Enfin, pour ce qui est du fait que le transporteur ait insisté pour que la plaignante remplisse en entier le formulaire à titre de *condition* du traitement de sa réclamation pour bagages perdus, nous avons constaté que les fins auxquelles les renseignements personnels étaient recueillis n'avaient pas été correctement indiquées, comme l'exige la *LPRPDE*. Nous avons également déterminé que la collecte du N°AS, de la date de naissance, de la profession et du nom de l'entreprise n'était pas nécessaire et nous sommes convaincus qu'une personne raisonnable n'estimerait pas acceptable que l'on recueille ces renseignements personnels dans ces circonstances.

arien :

- apporte les changements convenus précédemment;
- désigne l'« adresse d'affaires », le « numéro de téléphone au travail », l'« adresse électronique » et le « numéro d'identification de grand voyageur » comme facultatifs;
- retire la « profession » et le « nom de l'entreprise » du formulaire;
- regroupe tous les renseignements facultatifs dans une même section du formulaire pour que les passagers puissent choisir de remplir ou non la section, ou de la remplir en partie seulement;
- spécifie que l'« adresse précédente » et le « numéro de téléphone précédent » sont demandés uniquement à des fins de vérification de réclamation;
- donne les instructions suivantes à ses agents des réclamations : dès qu'un passager déclare une perte de bagages, lui expliquer quelle utilisation sera faite des renseignements personnels et préciser que les renseignements seront entrés dans un système de recherche, devenant ainsi accessibles aux autres utilisateurs du système; limiter la demande initiale aux renseignements justifiables aux stricts fins du but premier de la collecte — c'est-à-dire rechercher les bagages perdus.

que certains des renseignements demandés étaient facultatifs; en outre, il semble que le transporteur aérien n'avait pas comme pratique d'en informer les demandeurs.

En discutant avec le transporteur aérien, le Commissariat est arrivé aux conclusions suivantes :

- il n'est pas approprié qu'une entreprise demande le NAS d'un client pour des fins d'identification;
- il n'est pas approprié de demander la profession d'une personne pour traiter une réclamation, pas plus que le « nom de l'entreprise »;
- la date de naissance et plusieurs autres renseignements demandés sur le formulaire devraient être indiqués comme facultatifs;
- l'objet de la demande de renseignements mentionné sur le formulaire devrait être révisé pour préciser que les renseignements personnels recueillis seront entrés dans un système de recherche accessible à d'autres utilisateurs et pour indiquer clairement que les renseignements sont également recueillis à des fins de vérification de réclamation.

Même si le transporteur aérien a accepté de réviser le formulaire de la manière proposée, de ne plus demander le NAS et d'indiquer que la date de naissance, le numéro du passeport et le nom apparaissant sur le passeport sont facultatifs, il n'était pas enclin à faire d'autres concessions.

Dans nos conclusions, nous avons déterminé que le transporteur aérien n'avait pas énoncé les fins pour lesquelles il recueillait des renseignements personnels de façon que la plaignante puisse raisonnablement comprendre de quelle manière les renseignements allaient être utilisés ou communiqués. À notre avis, le transporteur aérien aurait dû indiquer clairement qu'à des fins de recherche des bagages, il devrait entrer les renseignements personnels dans un système de recherche, ce qui créerait un risque de communication aux autres utilisateurs du système. Nous avons indiqué que le transporteur aérien aurait également dû expliciter que « aux fins de la demande » signifie vérifier la réclamation et y donner suite. La formulation vague des « fins » ne constituait pas, en soi, un effort raisonnable de la part de l'entreprise pour aviser la plaignante des fins auxquelles ses renseignements personnels allaient servir ou être communiqués.

En ce qui concerne l'agence au comptoir qui a recueilli les renseignements personnels de la plaignante, nous avons déterminé qu'elle n'avait fait aucun effort pour lui expliquer comment on allait utiliser ces renseignements. Bien que l'agence ait très bien pu avoir

Même si nous avons établi que la plainte était fondée, nous avons salué l'initiative de l'entreprise d'avoir envoyé une lettre d'excuse au plaignant pendant l'enquête.

INDIQUER L'OBJET DE LA COLLECTE DES RENSEIGNEMENTS PERSONNELS

Les bagages que nous emportons

Aperçu

Elle voulait tout simplement que l'on retrouve ses bagages. Elle ne s'attendait sûrement pas à ce que, pour ce faire, le transporteur aérien fautive la demande d'indiquer son NAS, sa date de naissance et sa profession sur le formulaire de réclamation pour bagages perdus.

Même si elle était réticente à fournir ces renseignements, la plaignante a fini par remettre le formulaire de réclamation pour bagages perdus dûment rempli afin que le transporteur aérien puisse traiter sa demande. Aucun des renseignements personnels demandés n'était indiqué comme facultatif. Le formulaire précisait deux motifs de collecte des renseignements : servir à la recherche des bagages et servir de fondement à une demande d'indemnité.

Mesures prises par le CPVP

Le formulaire ne précisait pas, mais notre enquête l'a révélé, que les renseignements personnels recueillis seraient intégrés dans un système de recherche dont se servent des entreprises de transport aérien partout dans le monde et qu'ils seraient par conséquent accessibles à des tiers. Il ne précisait pas non plus que l'expression « aux fins d'une demande d'indemnité » ne signifiait pas seulement traiter la demande, mais aussi faire enquête sur la crédibilité de la plaignante.

Le Commissariat a appris que le système de recherche comprend un module d'enquête à l'aide duquel, à la suite d'une recherche infructueuse de bagages perdus, le transporteur aérien peut contrôler par recoupement toute réclamation antérieure ou toute information suspecte pouvant indiquer une intention malhonnête de la part d'un demandeur. Le transporteur aérien a reconnu que la plupart des renseignements recueillis au moyen de son formulaire servaient autant à vérifier les réclamations qu'à tenter de retrouver les bagages. Il a insisté sur le fait que les renseignements demandés n'étaient pas tous obligatoires, que les demandeurs étaient libres de refuser de fournir un renseignement s'ils n'étaient pas à l'aise de le faire. Cependant, il n'était écrit nulle part sur le formulaire

que l'accès à tout ordinateur grâce auquel on peut obtenir des renseignements personnels sur des clients soit restreint au personnel autorisé de la banque;

- prenne les mesures appropriées pour s'assurer que les clients ne puissent pas voir les mots de passe ou autres données d'identification utilisés par les employés pour l'ouverture d'une session.

Le Commissariat assure actuellement le suivi auprès de l'organisation pour s'assurer que les recommandations ont été mises en œuvre.

Perdu et retrouvé

Appercu

Un employé d'une entreprise s'est plaint auprès du Commissariat qu'un collègue de travail a trouvé une lettre le concernant dans un cartable de référence. Ce cartable était réservé aux employés et accessible à quiconque se trouvait sur le lieu de travail. La lettre résumait une réunion qui avait eu lieu quelque six ans auparavant entre le plaignant et ses supérieurs et où il était question des problèmes qu'il éprouvait au travail. La lettre recommandait une nouvelle affectation ainsi que certaines mesures qui aideraient le plaignant à surmonter nombre de problèmes personnels qu'il vivait à cette époque. Deux lettres se rapportant à deux autres employés ont également été trouvées au même endroit. Ces documents portaient sur des difficultés personnelles que ceux-ci éprouvaient au travail.

L'entreprise n'a pas été en mesure d'expliquer comment ces lettres ont abouti dans un cartable de référence et a suggéré que le cartable avait pu être mal rangé ou déplacé, puis rouvert plusieurs années plus tard. Nous avons constaté que le traitement que l'entreprise réserve aux documents contenant des renseignements personnels avait changé du tout au tout au cours des dernières années.

Mesures prises par la CPVP

À notre avis, des renseignements personnels d'une si grande sensibilité qui portent sur les problèmes personnels d'un employé requièrent une protection toute particulière. Bien que l'enquête n'ait pu établir comment ces lettres ont abouti dans le cartable, nous avons déterminé qu'il existait des lacunes au chapitre des mesures de sécurité prises par l'entreprise pour protéger les renseignements personnels des employés. Nous avons également remarqué que la période de conservation de ces documents était beaucoup plus longue que celle nécessaire pour répondre aux fins indiquées par l'entreprise.

plaignante était une directive énoncée dans un manuel de sécurité, enjoignant les employés de fermer l'ordinateur lorsqu'ils s'approprient à laisser l'appareil sans surveillance.

- Le simple fait qu'un employé de la banque ait négligé de suivre cette directive a, de fait, eu pour conséquence un accès non autorisé, par la plaignante, à des renseignements personnels sensibles.

- Bien qu'aucune communication inappropriée à un tiers n'ait eu lieu, le fait que l'employé ait négligé de suivre la directive a aussi donné lieu à un risque important d'une telle communication.

Dans les circonstances, les mesures de sécurité auxquelles se fiait la banque n'étaient ni efficaces ni appropriées. Nous estimons donc que la banque n'a pas respecté l'exigence prévue par la *LPRPDÉ* de fournir des mesures de protection appropriées.

Pour ce qui est des mesures correctives prises par la banque, nous estimons que, même si la fermeture automatique de l'écran de l'ordinateur représente sans nul doute une amélioration, elle n'en empêche pas l'accès pendant un laps de temps de 15 minutes et, par conséquent, ne peut pas être considérée comme une mesure de sécurité adéquate. Ce qui s'imposait était une mesure de sécurité protégeant les renseignements personnels sensibles en tout temps.

Quant à la seconde mesure corrective, nous constatons que, même si l'employé absent lors de l'incident connaissait la règle, il a omis de s'y conformer. En tenant compte du facteur humain, nous ne sommes pas convaincus qu'une directive plus ferme enjoignant les employés de clore la session serait susceptible d'être, de quelque façon, plus efficace que la première. Nous craignons même que le fait de se fier à une fonction de fermeture automatique après 15 minutes d'attente amènerait les employés à s'en contenter et qu'ils seraient moins portés à clore la session manuellement.

Nous estimons que les ordinateurs installés dans des aires ouvertes au public demeurent un risque inacceptable d'accès non autorisé à des renseignements personnels.

Nous recommandons que la banque :

- revoie ses politiques et mesures de sécurité en matière d'information applicables à ses succursales établies en magasin et prenne les mesures appropriées pour s'assurer

succursale ce jour-là, mais l'un n'était pas à son poste au moment de l'incident et l'autre s'occupait d'un client dans le bureau fermé.

La banque a qualifié l'incident de simple erreur humaine. Le dernier employé à avoir utilisé l'ordinateur installé dans l'aire ouverte avait omis de clore la session avant de laisser l'appareil sans surveillance, ce qui constitue une infraction à la politique et aux procédures de la banque en matière de sécurité.

Pour donner suite à la plainte, la banque a pris deux mesures correctives. D'abord, elle a fait parvenir un avis aux employés de succursales établies en magasin, affiché un message sur son site Intranet et ajouté quelques lignes directrices officielles dans les manuels de formation à l'intention des nouveaux employés. Ensuite, elle a installé un nouveau système informatique avec fonction de sécurité intégrée, c'est-à-dire un écran de veille protégé par mot de passe et qui s'active automatiquement si le clavier reste inactif pendant 15 minutes.

Pour ce qui est de l'allégation de la plaignante qu'elle avait pu reconnaître des caractères en clair dans le mot de passe de l'employé, la banque a indiqué que, avec le système informatique en usage au moment de l'incident, les mots de passe apparaissaient sous la forme de symboles, et non pas de caractères en clair. La banque a émis l'hypothèse que la plaignante avait soit pris le code d'usager de l'employé ou d'autres données servant à l'ouverture de session pour le mot de passe de celui-ci, ou encore avait reconnu des caractères en clair à partir du clavier au lieu de l'écran de l'ordinateur.

La plaignante a pour sa part soutenu que, peu importe comment les caractères ont été aperçus, les employés de la banque qui procèdent à une ouverture de session ne devraient pas laisser les clients voir l'écran ou le clavier d'ordinateur.

Mesures prises par le CFPV

Nous estimons que la plainte est fondée. Nous avons signalé que, avec sa pratique qui consistait à installer dans les aires ouvertes de ses succursales établies en magasin des ordinateurs souvent laissés sans surveillance, la banque avait pris un risque considérable d'accès non autorisé aux renseignements personnels de nature délicate des clients. À la question de savoir si la banque avait instauré des mesures de sécurité appropriées pour limiter ce risque et protéger les renseignements en question, nous avons déterminé ce qui suit :

- Au moment de l'incident, la première mesure de sécurité à laquelle la banque s'était fiée pour protéger les renseignements sensibles relatifs aux comptes de la

La succursale en question dispose d'un guichet automatique à l'usage du public, un bureau fermé muni d'un terminal d'ordinateur réservé à l'usage des employés, ainsi qu'un autre terminal d'ordinateur installé dans une aire ouverte mais également réservé à l'usage des employés et ce, bien qu'il n'y ait eu aucun avis à cet effet. Deux employés travaillaient à la banque, elle a soumis le cas à notre attention.

Plus tard, lorsqu'elle était en compagnie d'un employé de la banque, elle a pu le voir entrer son mot de passe, qui, prétend-elle, était affiché en toutes lettres sur l'écran lorsqu'il a ouvert une session sur un autre ordinateur. (Elle affirme que l'écran était placé de manière à ce qu'elle puisse le voir.) Inquiète du manque patent de mesures de protection prises par l'ordinateur ne lui avait pas demandé de mot de passe ni de code d'utilisateur.

Une cliente voulait faire quelques transactions dans une succursale bancaire située dans un supermarché. Pendant qu'elle attendait, elle a aperçu un ordinateur dans une aire ouverte. Voyant que l'écran était allumé et pensant que l'appareil visait à fournir au public des renseignements bancaires de nature générale, elle a tapé son nom et son adresse, tel que demandé. L'ordinateur a ainsi affiché un écran de renseignements relatifs à ses comptes à la banque, y compris ses numéros de carte de crédit, ses limites de crédit et ses soldes. L'ordinateur ne lui avait pas demandé de mot de passe ni de code d'utilisateur.

Alperçu

Beaucoup plus que des fruits et des légumes

Bien qu'il soit isolé, cet incident constitue un exemple des graves conséquences que la communication de renseignements personnels peut avoir pour les gens, qu'elle soit fortuite ou faite avec les meilleures intentions du monde.

Nous avons signalé qu'il est contraire à la politique de la banque qu'une personne se présente comme « l'intermédiaire » d'une tierce personne sans l'autorisation écrite de cette dernière. En raison de l'absence de document attestant l'autorisation de l'étudiant de communiquer les renseignements, nous étions d'avis que la banque ne s'était pas conformée à l'exigence d'obtenir le consentement prévu par la *Loi* et conclu que la plainte était fondée.

Mesures prises par le CPVP

des documents en son nom, avait formulé un commentaire à l'effet qu'elle faisait office d'« intermédiaire ». L'employée a fait savoir qu'à l'avenir, elle s'assurerait d'avoir en main un document signé attestant qu'une personne agit au nom d'une autre personne avant de discuter des renseignements personnels de quiconque.

Abandonnée : l'enquête s'est terminée avant que toutes les allégations soient pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, lesquels sont essentiels pour arriver à une conclusion.

Hors du secteur de compétence : l'enquête a montré que la LRPDE ne s'applique pas à l'organisation ou à l'activité faisant l'objet de la plainte.

Résolue hâtivement : le Commissariat a commencé à utiliser cette nouvelle disposition en 2004 pour traiter des situations où l'affaire est résolue avant même qu'une enquête officielle ne soit entamée. À titre d'exemple, si le sujet de la plainte déposée par une personne a déjà fait l'objet d'une enquête par le Commissariat et a été jugé conforme à la LRPDE, nous lui expliquons la situation. Cette conclusion est également utilisée lorsqu'une organisation, mise au courant des allégations, règle immédiatement la question à la satisfaction du plaignant et du Commissariat.

Cas choisis en vertu de la LRPDE

PROTECTION DES RENSEIGNEMENTS PERSONNELS

Déprime nuptiale

Aperçu

Elle croyait tout simplement se rendre utile. C'est sans aucun doute ce qu'une employée de banque a pensé lorsqu'elle a remis à la fiancée d'un client une copie de la demande de prêt étudiant de ce dernier, laquelle renfermait de l'information de l'année précédente concernant ses emprunts et sa carte de crédit. Elle croyait que ces renseignements aideraient son client à remplir le formulaire pour le nouveau trimestre scolaire et qu'il n'y avait rien de mal à laisser son dossier sur son bureau, à la vue de la fiancée, lorsqu'elle est allée chercher un autre document.

Ce ne fut pas le cas. La jeune femme savait que son ami avait un prêt étudiant mais elle ne connaissait le montant intégral de la dette jusqu'à ce qu'elle voit le dossier. Elle a alors annulé le mariage.

L'employée a reconnu son erreur. Elle croyait que la fiancée faisait office d'agent de son client parce que la jeune femme, qui s'était rendue à la banque pour y remettre

ENQUÊTES ET DEMANDES DE RENSEIGNEMENTS

Le Commissariat a reçu 302 plaintes en vertu de la LPRPDE entre le 1^{er} janvier et le 31 décembre 2003, soit à peu près le même nombre qu'en 2002. Comme par le passé, les plaintes ont été déposées contre toute une gamme d'organisations et ont porté sur des allégations d'atteinte aux droits à la vie privée. De nouveau, le plus grand nombre de plaintes (42 %) a visé des organisations du secteur bancaire. Le pourcentage de plaintes à l'encontre d'organisations du secteur des télécommunications et de la radiodiffusion s'est établi à 26 %, tandis que celui des plaintes contre les sociétés de transport a enregistré une légère hausse, pour passer à 19 %. Les plaintes contre les agences d'évaluation du crédit ont compté pour 4 % du total, le solde (9 %) faisant intervenir des programmes de récompenses, des fournisseurs de service Internet et des conseils de bandes autochtones.

Le nombre de cas clos en 2003 est passé à 278, soit une hausse de 58 % par rapport à l'an dernier. Les conclusions suivantes ont été rendues :

Non fondées	115	(41 %)
Fondées	97	(35 %)
Résolues	14	(5 %)
Résolues en cours d'enquête	4	(2 %)
Hors du secteur de compétence	5	(2 %)
Abandonnées	43	(15 %)

Définitions des conclusions en vertu de la LPRPDE

Non fondée : l'enquête n'a pas permis de déceler des éléments de preuves qui suffisent à conclure qu'une organisation a enfreint les droits du plaignant en vertu de la LPRPDE.

Fondée : l'organisation n'a pas respecté une disposition de la LPRPDE.

Résolue : l'enquête a corroboré les allégations, mais l'organisation a pris les mesures nécessaires pour remédier à la situation, à la satisfaction du Commissariat, ou s'est engagée à prendre ces mesures correctives.

Résolue au cours de l'enquête : le Commissariat a aidé à négocier une solution qui satisfait toutes les parties en cause au cours de l'enquête. Aucune conclusion n'a été rendue.

Rapport concernant la Loi sur la protection des renseignements personnels et les documents électroniques

INTRODUCTION

La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) établit les règles de base sur la façon dont les organisations du secteur privé peuvent recueillir, utiliser et communiquer les renseignements personnels dans le cadre de leurs activités commerciales.

Depuis son entrée en vigueur le 1^{er} janvier 2001, la *Loi* s'est principalement appliquée aux activités commerciales de ce qu'on appelle les installations, les ouvrages, les entreprises ou les secteurs d'activité fédéraux, tels que les entreprises de transport et de télécommunications, les banques et les radiodiffuseurs. Elle s'applique également aux renseignements personnels des employés de ces entreprises, ainsi qu'à la vente, à la location ou au troc de renseignements personnels au-delà des frontières provinciales ou nationales par des organisations sous réglementation provinciale.

Depuis le 1^{er} janvier 2002, les renseignements personnels sur la santé recueillis, utilisés ou communiqués par ces organisations sont aussi assujettis à la *Loi*.

Depuis le 1^{er} janvier 2004, la *LPRPDE* porte sur la collecte, l'utilisation ou la communication de renseignements personnels dans le cadre de toutes les activités commerciales au Canada, sauf dans le cas de la collecte, de l'utilisation et de la communication de renseignements personnels à l'intérieur des provinces ayant adopté des lois essentiellement similaires.

La *LPRPDE* s'applique également à la collecte, à l'utilisation et à la communication des renseignements transfrontaliers ainsi qu'aux installations, ouvrages, entreprises ou secteurs d'activité fédéraux.

A de nombreuses reprises, le Commissaire est intervenu dans d'autres litiges ne visant pas la *Loi sur la protection des renseignements personnels* à l'égard desquels des interprétations de la *Loi* ont été présentées.

Dans le rapport annuel de l'an dernier, nous avons signalé la conclusion d'un certain nombre d'affaires auxquelles le Commissaire a participé activement. Au cours du dernier exercice, aucun litige important concernant l'interprétation de la *Loi sur la protection des renseignements personnels* n'a exigé l'intervention du CPVP.

retards dans la transmission de commentaires aux ministères. Le CPVP est résolu à combler cet écart au chapitre des ressources et croit bien qu'il arrivera à trouver une solution à ce problème.

Nous sommes d'avis qu'aucune autre initiative gouvernementale depuis la promulgation de la *Loi sur la protection des renseignements personnels* en soi n'a contribué autant à favoriser une culture respectueuse de la vie privée dans la fonction publique fédérale.

Il n'en demeure pas moins que le Commissariat estime qu'il a dû relever un défi de taille en s'acquittant de son rôle de conseiller prévu par la *Politique de l'évaluation des facteurs relatifs à la vie privée* sans pour autant recevoir de ressources supplémentaires. En raison du manque de ressources humaines et financières à cette fin et de l'importante augmentation du volume des présentations au cours de cet exercice, de malencontreux retards ont été signalés dans l'émission des commentaires dont les ministères ont besoin. Le CPVP s'efforcera de trouver une solution à ce déficit au chapitre des ressources de manière à éviter d'autres retards, à rattraper l'arriéré actuel et à fournir aux ministères un soutien adéquat aux fins de l'application de la *Politique d'évaluation des risques relatifs à la vie privée* du SCT.

DEVANT LES TRIBUNAUX

Aux termes de l'article 41 de la *Loi sur la protection des renseignements personnels*, une personne est autorisée, à l'issue d'une enquête par le Commissaire à la protection de la vie privée, à déposer auprès de la Cour fédérale du Canada un recours en révision d'une décision d'une institution fédérale qui lui a refusé l'accès à ses renseignements personnels. Depuis l'entrée en vigueur de la *Loi sur la protection des renseignements personnels* en 1983 jusqu'au 31 mars 2004, environ 141 recours en révision ont été déposés devant la Cour fédérale. De ce nombre, 11 ont été déposés au cours de l'exercice qui a pris fin le 31 mars 2004.

L'article 42 de la *Loi sur la protection des renseignements personnels* autorise le Commissaire à comparaître devant la Cour fédérale. Le Commissaire peut exercer lui-même un recours en révision de la décision d'une institution fédérale qui a refusé l'accès à des renseignements personnels, dans la mesure où il obtient le consentement de la personne qui a demandé les renseignements. Il peut également comparaître devant la Cour au nom d'une personne qui a exercé le recours devant elle en vertu de l'article 41 ou comparaître, avec l'autorisation de la Cour, comme partie à une instance engagée en vertu de l'article 41.

du Commissaire pour l'exercice 2002-2003 contient la liste des erreurs et omissions communes que nous avons remarquées lors de ces premières présentations.

Nous avons cependant constaté des améliorations marquées du caractère complet et de la qualité des EFVP et EPPFVP que nous avons reçues au cours du dernier exercice. Nous estimons que ces améliorations témoignent des enseignements que les ministères tirent de leurs consultations avec le Commissariat. Elles peuvent également être

attribuées aux efforts déployés par le Secréariat du Conseil du Trésor pour informer les ministères sur les exigences et les méthodologies préconisées par la *Politique L*.¹ « outil d'apprentissage en ligne pour l'EFVP » du Conseil du Trésor, disponible en direct depuis l'automne 2003, constitue une ressource précieuse à ce chapitre. Nous recommandons à quiconque veut en savoir davantage sur le processus de l'EFVP de consulter le site Web du Conseil du Trésor à l'adresse www.tbs-sct.gc.ca.

Perspectives d'avenir

Bien que nous applaudissions à l'amélioration générale des présentations des EFVP et des EPPFVP que nous avons reçues, nous continuons de nous inquiéter d'une omission fréquente. En effet, nombre d'EFVP ne contiennent pas de plan d'action permettant de réduire les risques pouvant compromettre le droit à la vie privée. Le Commissariat collaborera avec les ministères et organismes pour les encourager à inclure de tels plans d'action dans toutes les EFVP et pour aider les ministères à déterminer les prochaines mesures qui s'imposent.

Toutefois, tout semble montrer que la *Politique* atteint son but principal, à savoir de sensibiliser davantage des fonctionnaires de tous les niveaux hiérarchiques à l'importance de la protection de la vie privée dans l'exercice de leurs fonctions administratives quotidiennes. Les ministères ne peuvent plus créer de nouvelles bases de données, lier des fonds de renseignements, conclure des ententes de partage des renseignements avec d'autres ministères ou lancer de nouveaux programmes ou services sans avoir pris en compte leur éventuelle incidence sur la vie privée.

À l'instar des ministères qui ont dû jongler avec des ressources restreintes pour se conformer aux exigences de la *Politique*, le CPVP, le CPVP a été tenu d'attribuer suffisamment de moyens pour bien s'acquitter du rôle de consultation que lui confère la *Politique* et ce, sans avoir reçu de ressources supplémentaires.

La réduction des effectifs du CPVP pouvant être affectés à l'examen des EFVP et EPPFVP, jumelée à une hausse du volume des présentations au cours du dernier exercice, a entraîné des

- la réforme des lois et des politiques;
- les risques sur la protection des renseignements suscités par des programmes et initiatives particuliers.

La Direction des examens et des pratiques en matière de vie privée aide aussi les organisations du secteur privé à évaluer les risques pouvant compromettre le respect de la vie privée, à inculquer des pratiques exemplaires et à élaborer des politiques convenables en matière de protection de la vie privée.

Évaluations des facteurs relatifs à la vie privée

La *Politique d'évaluation des facteurs relatifs à la vie privée* (EFVP) du Secrétaire du Conseil du Trésor du Canada est en vigueur depuis mai 2002. Lorsqu'elle a été instaurée, les membres de la collectivité des professionnels de la protection de la vie privée l'ont accueillie avec enthousiasme, et ce, avec raison. Pour la première fois, les ministères et organismes fédéraux étaient dotés d'un outil leur permettant de prévoir l'incidence sur la vie privée d'une initiative donnée, d'évaluer et de pondérer cette incidence avec uniformité et de concevoir des stratégies d'atténuation de cette incidence ou de ces risques. En exigeant que les principes en matière de protection de la vie privée soient pris en compte aux étapes de la planification, de la conception et de la mise en œuvre, la *Politique* permet de donner corps à ces principes et de les officialiser.

La *Politique* est la première du genre à rendre les EFVP obligatoires pour l'ensemble des nouveaux programmes et services du gouvernement fédéral qui pourraient soulever des enjeux en matière de protection de la vie privée. Elle exige des ministères et organismes fédéraux qu'ils informent le Commissaire à la protection de la vie privée lorsqu'ils effectuent une EFVP, ce qui donne au CPVP l'occasion d'examiner et de commenter ce projet. Cela fournit une assurance accrue que les risques liés à une initiative donnée ont été dûment identifiés et que les mesures proposées pour atténuer ces risques sont raisonnables et appropriées.

Point de vue du CPVP sur les EFVP

Depuis l'entrée en vigueur de la *Politique* en mai 2002, plus de 100 rapports d'EFVP et d'évaluations préliminaires des facteurs relatifs à la vie privée (EPFVP) ont été soumis au CPVP à des fins d'examen. Le caractère complet et la qualité de nombre des EFVP et EPFVP (évaluations) présentées la première année étaient très variés, ce qui est habituel lorsqu'une nouvelle directive stratégique est adoptée. Le Rapport annuel

- un guide de vérification des évaluations des facteurs relatifs à la vie privée;
- des politiques d'appariement des données;
- des politiques d'utilisation du numéro d'assurance sociale (NAS);
- des pratiques exemplaires en matière de vie privée à l'intention des ministères;

Les consultations ont porté sur un vaste éventail de sujets, notamment :

services frontaliers du Canada.

Affaires indiennes et du Nord Canada, l'Agence du revenu du Canada et l'Agence des services frontaliers du Canada.

Santé Canada, Ressources humaines et Développement des compétences Canada, nombreux ministères fédéraux dont le Conseil du Trésor du Canada, Statistique Canada, au besoin des conseils, commentaires et recommandations à caractère moins officiel à de La Direction des examens et des pratiques en matière de vie privée fournit également

Autres consultations et services consultatifs

à la protection de la vie privée.

obligations prévues à l'article 7 de la Loi et à préparer leurs présentations au Commissariat

ressources à l'élaboration d'un guide qui aidera les organisations à comprendre leurs

particulièrement problème. Lors du prochain exercice, le Commissariat consacrera des

pratiquement impossible à obtenir » et les circonstances entourant cette situation posent

de l'alinéa 7(3) de la LPRPD. La question de savoir quand « le consentement est

est évident que les organisations ne connaissent pas bien leurs obligations aux termes

la qualité de ces présentations variaient. Même si notre échantillon est très petit, il

de renseignements médicaux à des fins de recherche en santé. Le caractère complet et

l'alinéa 7(3) de la LPRPD, dont la plupart portent sur l'utilisation et la communication

Au cours du dernier exercice, le Commissariat a reçu quatre avis conformément à

renseignements soient utilisés d'une manière qui en assure le caractère confidentiel.

communiquer les renseignements a pris les mesures nécessaires pour veiller à ce que les

3) le « consentement est pratiquement impossible à obtenir » et 4) l'organisation qui

être atteint sans que les renseignements ne soient fournis sur un support identifiable,

à des fins d'étude ou de recherche étudites », 2) l'objet de la communication ne peut

dont la communication est envisagée serviront uniquement » à des fins statistiques ou

Dans leurs présentations, les organisations doivent montrer que : 1) les renseignements

leurs activités commerciales respectives.

sur l'application des principes des pratiques exemplaires de la protection de la vie privée à

à servir de ressource aux organisations du secteur privé à la recherche de renseignements

Notre rôle consiste à fournir des services consultatifs à nombre de ministères fédéraux et

et la *LPRPD*, tandis que d'autres sont visées par des politiques du gouvernement fédéral. D'autres activités d'examen ont découlé d'accords institutionnels comportant la consultation volontaire du Commissariat au sujet de questions liées à la protection de la vie privée. Tel est notamment le cas du Comité du protocole de gouvernance des banques de données de Ressources humaines et Développement des compétences Canada (RHDC) — anciennement Développement des ressources humaines Canada (DRHC).

Examen de la banque de données de RHDC

Comme nous l'avons décrit dans nos rapports antérieurs, RHDC a établi un processus d'examen pour traiter des activités d'analyse, de recherche et d'évaluation des politiques qui comportent la connexion de banques de données distinctes. Une partie de ce processus comprend une consultation avec le Commissariat. Au cours de la dernière année, le Commissariat a analysé et commenté 20 présentations de RHDC, dont l'évaluation du programme d'assurance-emploi depuis les réformes de 1996, le succès connu par diverses ententes sur le développement du marché du travail et des études portant sur le Programme canadien des prêts aux étudiants. Depuis plusieurs années, nous avons été témoins d'une amélioration marquée du caractère exhaustif et de la qualité des présentations que nous avons reçues. Cela témoigne de l'importance que RHDC accorde à ses activités de connexion des données et de son dévouement afin de faire en sorte que cette connexion s'effectue en conformité des principes de pratiques exemplaires en matière de protection de la vie privée.

Politique de couplage des données

Conformément à la *Politique sur le couplage des données* du Secrétariat du Conseil du Trésor, il incombe aux ministères et organismes fédéraux d'informer le Commissariat de toute proposition de couplage des données. Cet avis a pour objet de donner au Commissariat la possibilité d'examiner et de commenter la proposition pour veiller à ce que le couplage des données soit conforme aux exigences de la *Politique*. Au cours du dernier exercice, le Commissariat a reçu 10 présentations relatives au couplage des données. Ces présentations étaient conformes aux exigences minimales de la *Politique*, mais nous avons dû rappeler aux ministères qu'ils avaient le devoir d'informer le public lorsqu'ils couplaient les renseignements personnels les concernant à d'autres fonds de renseignements détenus par le gouvernement. Dans la plupart des cas, un tel avis ne porte pas préjudice à l'utilisation des renseignements.

Communication à une tierce personne de renseignements personnels

Conformément aux alinéas 7(2)(c) et 7(3)(f) de la *LPRPD*, les organisations du secteur privé sont tenues d'informer le Commissariat lorsque des renseignements personnels sont communiqués à une tierce personne sans le consentement de l'intéressé « à des fins statistiques ou à des fins d'étude ou de recherche étudites ».

Outre les vérifications de la conformité, le Commissariat examine les présentations d'organisations du secteur public fédéral et du secteur privé et offre des conseils sur un vaste éventail de questions en matière de conformité. Certaines de ces activités d'examen de la conformité sont prévues par la *Loi sur la protection des renseignements personnels*

Autres activités de conformité

Ces changements permanents ont touché certaines des observations et constatations contenues dans notre rapport de 2001 ainsi que celles de notre plus récent examen. Cela dit, compte tenu de l'état actuel de la situation, nous avons fait progresser passablement le dossier du règlement des questions laissées en suspens par le Centre canadien des armes à feu. Nous signalerons les éventuels progrès dans le rapport annuel de l'an prochain.

Notre examen du programme des armes à feu a été rendu plus complexe en raison, notamment, du fait que le programme en soi est une véritable cible en mouvement étant donné les changements constants dont il a fait l'objet sur le plan de la législation, des politiques, de l'administration et de la technologie de l'information (TI). Cette dernière année, par exemple, la vérificatrice générale a déposé son rapport sur l'optimisation des ressources du programme dans lequel elle recommandait que des changements lui soient apportés. La responsabilité du programme est passée du ministre de la Justice au Solliciteur général (ministère qui est devenu Sécurité publique et Protection civile Canada — SPPCC), un nouveau poste de Commissaire aux armes à feu a été créé, le Parlement a adopté le projet de loi C-10 et, en janvier 2004, on a confié à la ministre Guarnieri le mandat d'examiner en profondeur le programme.

Le Programme canadien de contrôle des armes à feu

Au cours de l'année, nous avons poursuivi notre examen minutieux du Programme canadien de contrôle des armes à feu, qui a fait l'objet d'un examen en 2001 par le Commissariat. Quelques-unes des recommandations que nous avons formulées en 2001 ont été mises en œuvre. À titre d'exemple, la GRC a adopté nos recommandations de 2001 qui visent à limiter l'accès des proposés aux armes à feu au Système de récupération des renseignements judiciaires (SIRJ) et aux dossiers opérationnels. Nous avons également assuré le suivi de nombreuses questions laissées en suspens que nous avions mentionnées dans notre rapport complet sur les armes à feu de 2001, tels l'impartition, les accords internationaux sur le partage de renseignements et le recours à des questionnaires supplémentaires.

nous entamons une vérification des activités de communication transfrontalière des renseignements de l'Agence des services frontaliers du Canada (ASFC).

Examens du SCRS et du CST

Il convient de signaler que les examens menés auprès du SCRS et du CST n'incluaient pas la formulation de commentaires sur les grandes questions concernant la sécurité nationale et les activités de collecte de renseignements. Les examens ont plutôt porté sur l'évaluation de l'incidence des mesures antiterroristes sur les pratiques de traitement des renseignements personnels de ces institutions. Nos enquêtes ont démontré que les événements du 11 septembre 2001 n'ont pas entraîné de changements de fond de la gestion des renseignements personnels détenus par le SCRS et le CST. Notre examen de documents choisis et les réponses fournies par les fonctionnaires du SCRS et du CST qui ont été consultés n'ont fait ressortir aucune question ni aucune préoccupation d'importance se rapportant à la *Loi sur la protection des renseignements personnels*.

Examens de la GRC

L'examen de la conformité mené auprès de la GRC a porté sur trois initiatives principales : celle relative aux équipes intégrées de sécurité nationale (EISN), celle relative aux équipes intégrées de la police des frontières (EIPF) et celle relative à la création du Bureau de renseignement financier. Bien que notre examen ait permis de déceler un niveau élevé de conformité avec la *Loi sur la protection des renseignements personnels*, nous nous sommes inquiétés des ententes ou des accords régissant le partage des renseignements personnels entre la GRC et ses partenaires membres des EISN et des EIPF. Cette question continue de faire l'objet de discussions avec la GRC.

Circulation transfrontalière des renseignements personnels

Nombre de programmes et d'activités établis par des institutions et organismes du gouvernement fédéral prévoient la communication de renseignements personnels sur des citoyens et des résidents canadiens à des départements et organismes des États-Unis. Au cours de cet exercice, le Commissariat a terminé un examen des accords, des ententes et des protocoles d'entente conclus entre le Canada et les États-Unis qui prévoient des dispositions pour la communication de renseignements personnels. Nous avons constaté que nombre de ces ententes ne contenaient pas de dispositions satisfaisantes de protection des renseignements personnels.

La circulation transfrontalière des renseignements personnels comporte de sérieux risques en matière de protection de la vie privée qui ont trait aux différences entre les secteurs de compétence qui influent sur la protection des renseignements personnels, la sécurité des renseignements personnels en transit et le caractère satisfaisant des mécanismes juridiques régissant la gestion des renseignements communiqués. Les enjeux liés à la circulation transfrontalière des renseignements personnels figureront parmi les principaux secteurs des examens que le Commissariat mènera au cours du prochain exercice. C'est pourquoi

établies dans la Loi sur la protection des renseignements personnels.

ainsi qu'évaluer le degré de conformité de la gestion des renseignements personnels en vertu des nouvelles initiatives avec les pratiques équitables en matière d'information 11 septembre 2001 qui influeraient sur le droit à la vie privée de la population canadienne nouvelles initiatives prévues ou mises en œuvre par les organisations au lendemain du Canada conformément à son plan de lutte contre le terrorisme, examiner les éventuelles SCRS à la suite de l'adoption des mesures antiterroristes par le gouvernement du des pouvoirs législatifs et des programmes opérationnels de la GRC, du CST et du Ces examens visaient les objectifs suivants : déterminer ce qui avait changé au chapitre sécurité (SCRS) et du Centre de la sécurité des télécommunications (CST).

de la Gendarmerie royale du Canada (GRC), du Service canadien du renseignement de Canadiens et des Canadiennes. Dans cette optique, nous avons mené des examens auprès antiterroristes prises au lendemain du 11 septembre 2001 sur le droit à la vie privée des été question dans le rapport annuel de l'an dernier, d'évaluer l'incidence des mesures Outre ces deux vérifications, le Commissariat a donné suite à l'engagement, dont il a ***Enquête sur la lutte contre le terrorisme***

ces deux institutions aux recommandations qu'ils contiennent. À la fin des examens, nous avons remis au CCRI et au CGFC des rapports contenant ces constatations. Nous venons de déposer nos rapports finaux et attendons les réponses de régissant l'utilisation des télécopieurs pour transmettre des renseignements personnels.

de l'objet de la collecte. De plus, l'examen a révélé la nécessité d'établir une politique personnels devaient être améliorés afin de veiller à ce que les personnes soient informées que certains des formulaires dont le Comité se sert pour recueillir des renseignements de pratiques équitables en matière de renseignements. Toutefois, nous avons remarqué de conformité avec la *Loi sur la protection des renseignements personnels* et ses principes Notre examen des opérations du Comité nous a permis de constater un niveau élevé ***Le Comité des griefs des Forces canadiennes***

forme les dossiers en respectant les échéanciers de conservation et de retrait établis. dossiers en fonction de leur cote de sécurité respective et veiller à retirer en bonne et due sont transportés hors des limites physiques du CCRI. En outre, il faudrait identifier les dossiers opérationnels et des renseignements contenus dans les ordinateurs portables qui autres, la nécessité d'élaborer des politiques et des protocoles concernant la protection des le Commissariat a décelé plusieurs secteurs exigeant des mesures correctrices, entre

Examens et vérifications aux termes de la

Loi sur la protection des renseignements personnels

Au cours de la dernière année, le Commissariat a procédé à des examens prévus à l'article 37 des pratiques de traitement des renseignements personnels du Conseil canadien des relations industrielles (CCRI) et du Comité des griefs des Forces canadiennes (CCGC). Nous avons choisi ces deux institutions non pas parce que nous soupçonnions une non-conformité avec les pratiques acceptables de protection de la vie privée, mais plutôt parce qu'il s'agit de petites institutions qui, par le passé, n'ont pas été soumises au même degré d'examen que l'ont été les grandes institutions fédérales détenant d'importants fonds de renseignements personnels.

Les examens menés auprès du CCRI et du CCGC visaient à fournir des conseils et de l'éducation en matière de protection de la vie privée. Ces éléments revêtent une importance particulière dans les institutions de petite taille qui ont des ressources relativement restreintes à consacrer à la protection de la vie privée. Nous nous sommes penchés sur les pratiques entourant la collecte, l'utilisation, la communication, la protection, la conservation et le retrait des renseignements personnels qui s'appliquent aux documents sur support papier et sur support électronique. Nous avons en outre examiné les listes publiques des institutions dans *Info Source*, leurs activités de passation de marchés, la sensibilisation des employés à leurs droits et obligations aux termes de la *Loi sur la protection des renseignements personnels*, les ententes de télétravail, la surveillance en milieu de travail et les questions de sécurité liées à la transmission des renseignements par voie électronique.

Le Conseil canadien des relations industrielles

Le CCRI, un tribunal indépendant quasi-judiciaire, est chargé d'interpréter et d'administrer la partie I (Relations du travail) et certaines dispositions de la partie II (Santé et sécurité au travail) du *Code canadien du travail*. Le Conseil accrédite les syndicats, fait enquête sur les pratiques déloyales de travail, ordonne la cessation des grèves et des lockouts illégaux, tranche des questions relatives aux secteurs de compétence, traite des points complexes des fusions et des ventes de sociétés et offre des services de médiation et d'arbitrage aux fins du règlement des différends.

L'examen de la conformité a été mené dans des locaux de l'administration centrale du CCRI à Ottawa et dans les bureaux régionaux à Toronto et à Vancouver. Il est ressorti de l'examen que les pratiques de traitement des renseignements personnels du Conseil étaient en général conformes aux principes de pratiques équitables en matière de renseignements établis aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels*. Toutefois,

Enquêtes terminées et résultats selon les répondants (suite)

Pour les plaintes terminées entre le 1^{er} avril 2003 et le 31 mars 2004

Répondants Abandon- Non Résolues Résolues Résolues Fondées Fondées Total
nées fondées au cours de l'enquête et résolues

Ombudsman de la	1	0	0	0	0	0	0	1
Défense nationale								
et des Forces								
canadiennes								
Bureau du Conseil	0	2	0	0	1	0	0	3
privé								
Commission de la	0	4	0	1	4	0	0	9
fonction publique								
du Canada								
Travaux publics	2	7	0	1	4	0	0	14
et Services								
gouvernementaux								
Canada								
Gendarmerie royale	4	79	1	25	52	3	164	
du Canada								
Solliciteur général	0	10	0	1	0	0	11	
Canada								
Statistique Canada	0	1	0	0	0	0	1	
Transports Canada	2	2	0	0	0	1	5	
Secrétariat du	0	4	2	0	2	0	8	
Conseil du Trésor du								
Canada								
Anciens combattants	0	1	0	0	2	0	3	
Canada								
Total	366	1 243	11	265	1 180	69	3 134	

EXAMENS ET PRATIQUES EN MATIÈRE DE VIE PRIVÉE

Le Commissariat à la protection de la vie privée promeut la conformité avec les deux lois sur la protection de la vie privée du Canada en exécutant des vérifications de la protection de la vie privée et des examens de la conformité. Il représente une source d'expertise interne fournissant aide et conseils aux institutions des secteurs public et privé. Depuis l'adoption de la *Politique d'évaluation des facteurs relatifs à la vie privée* (EFVP) du Secrétaire du Conseil du Trésor en mai 2002, le Commissariat a assumé la responsabilité d'examiner et de commenter les EFVP préparées par les institutions fédérales.

Enquêtes terminées et résultats selon les répondants (suite)

Pour les plaintes terminées entre le 1^{er} avril 2003 et le 31 mars 2004

Répondants	Abandon- nées	Non fondées	Résolues	Résolues au cours de l'enquête	Fondées	Fondées et résolues	Total
Santé Canada	0	481	0	4	2	1	488
Développement des ressources humaines	1	25	1	9	9	6	51
Commission de l'immigration et du statut de réfugié	0	3	0	1	10	4	18
Affaires indiennes et du Nord Canada	0	2	0	1	0	0	3
Industrie Canada	0	6	0	0	1	0	7
Justice Canada, ministère de la	0	7	0	41	7	1	56
Commission d'examen des plaintes concernant la police militaire	0	4	0	0	0	0	4
Autorité portuaire de Montreal	0	1	0	0	0	0	1
Autorité portuaire de Nanaimo	0	0	1	0	0	0	1
Archives nationales du Canada	0	0	0	1	2	0	3
Défense nationale	7	21	0	19	52	10	109
Commission nationale des libérations	2	19	0	0	2	0	23
Conseil national des recherches du Canada	1	2	0	0	1	0	4
Ressources naturelles Canada	0	1	0	0	0	0	1
Conseil de recherches en sciences naturelles et en génie du Canada	0	1	0	0	0	0	1
Bureau du surintendant des institutions financières du Canada	0	2	0	0	0	0	2

Enquêtes terminées et résultats selon les répondants (suite)

Pour les plaintes terminées entre le 1^{er} avril 2003 et le 31 mars 2004

Répondants	Abandon- nées	Non fondées	Résolues	Résolues au cours de l'enquête	Fondées	Fondées et résolues	Total
Commission canadienne des droits de la personne	0	0	0	0	1	0	1
Agence canadienne de développement international	0	1	0	0	0	0	1
Musée canadien des civilisations	3	0	0	0	0	0	3
Conseil de la radiodiffusion et des télécommunications canadiennes	0	2	0	2	0	0	4
Service canadien du renseignement de sécurité	1	43	0	4	0	0	48
Agence spatiale canadienne	0	0	0	0	1	0	1
Citoyenneté et Immigration Canada	12	25	0	13	41	1	92
Commission des plaintes du public contre la GRC	0	1	0	0	0	0	1
Commissariat aux langues officielles	0	0	0	0	1	0	1
Communication Canada	0	1	0	0	0	0	1
Enquêteur correctionnel	0	0	0	0	4	0	4
Service correctionnel Canada	308	357	2	46	911	12	1 636
Environnement Canada	3	1	0	2	0	0	6
Finances Canada, ministère des	0	1	0	0	0	0	1
Pêches et Océans	2	5	0	3	0	1	11
Affaires étrangères et Commerce international	3	6	1	5	1	0	16
Canada							

Enquêtes terminées selon le répondant (suite)

Pour les plaintes reçues entre le 1^{er} avril 2003 et le 31 mars 2004

Conseil national des recherches du Canada	4
Ressources naturelles Canada	1
Conseil de recherches en sciences naturelles et en génie du Canada	1
Bureau du surintendant des institutions financières du Canada	2
Ombudsman de la Défense nationale et des Forces canadiennes	1
Bureau du Conseil privé	3
Commission de la fonction publique Canada	9
Travaux publics et Services gouvernementaux Canada	14
Gendarmerie royale du Canada	164
Solliciteur général du Canada	11
Statistique Canada	1
Transports Canada	5
Secrétariat du Conseil du Trésor du Canada	8
Anciens combattants Canada	3
Total	3 134

Enquêtes terminées et résultats selon les répondants

Pour les plaintes terminées entre le 1^{er} avril 2003 et le 31 mars 2004

Répondants	Abandon- nées	Non fondées	Résolues	Résolues au cours de l'enquête	Fondées	Fondées et résolues	Total
Agriculture et Agroalimentaire Canada	1	1	0	2	2	0	6
Banque du Canada	0	0	0	1	0	0	1
Banque de développement du Canada	0	1	0	0	0	0	1
Agence des douanes et du revenu du Canada	5	94	2	65	60	26	252
Société canadienne des postes	7	14	1	14	7	3	46
Centre canadien des armes à feu	0	1	0	2	0	0	3
Agence canadienne d'inspection des aliments	1	2	0	0	1	0	4
Patrimoine canadien	0	2	0	1	0	0	3

Enquêtes terminées selon le répondant

Pour les plaintes reçues entre le 1^{er} avril 2003 et le 31 mars 2004

Institutions fédérales

6	Agriculture et Agroalimentaire Canada
1	Banque du Canada
1	Banque de développement du Canada
252	Agence des douanes et du revenu du Canada
46	Société canadienne des postes
3	Centre canadien des armes à feu
4	Agence canadienne d'inspection des aliments
3	Patrimoine canadien
1	Commission canadienne des droits de la personne
1	Agence canadienne du développement international
1	Musée canadien des civilisations
4	Conseil de la radiodiffusion et des télécommunications canadiennes
48	Service canadien du renseignement de sécurité
1	Agence spatiale canadienne
92	Citoyenneté et Immigration Canada
1	Commission des plaintes du public contre la GRC
1	Commissariat aux langues officielles
1	Communication Canada
4	Enquêteur correctionnel du Canada, Bureau de l'
1 636	Service correctionnel Canada
6	Environnement Canada
1	Finances Canada, ministère des
11	Pêches et Océans
16	Affaires étrangères et Commerce international Canada
488	Santé Canada
51	Développement des ressources humaines Canada
18	Commission de l'immigration et du statut de réfugié
3	Affaires indiennes et du Nord Canada
7	Industrie Canada
56	Justice Canada, ministère de la
4	Commission d'examen des plaintes concernant la police militaire
1	Autorité portuaire de Montréal
1	Autorité portuaire de Nainimo
3	Archives nationales du Canada
109	Défense nationale
23	Commission nationale des libérations conditionnelles

Enquêtes terminées selon le lieu d'origine

Pour les plaintes terminées entre le 1er avril 2003 et le 31 mars 2004

Provinces et territoires		Total
Alberta	658	
Colombie-Britannique	1 128	
International	18	
Manitoba	65	
Région de la capitale nationale (Ontario)	140	
Région de la capitale nationale (Québec)	22	
Nouveau-Brunswick	41	
Terre-Neuve	8	
Nouvelle-Écosse	27	
Nunavut	1	
Ontario	315	
Île-du-Prince-Édouard	1	
Québec	560	
Saskatchewan	150	
Total	3 134	

Plaintes selon le type de plaintes et leur résultat

Pour les plaintes terminées entre le 1er avril 2003 et le 31 mars 2004

Abandon- nées	Non fondées	Résolues	Résolues au cours de l'enquête	Fondées	Fondées et résolues	Total
Accès	40	477	6	177	19	782
Collecte	6	503	3	14	12	539
Correction — annotation	0	10	0	2	0	14
Correction — Délais	1	1	0	0	14	16
Avis de prorogation	0	16	0	0	14	30
Frais inexact	1	0	0	0	0	1
Langue	0	2	0	0	0	2
Conservation et retrait	1	5	0	6	1	15
Délais	294	140	0	11	1 066	1 511
Utilisation et communi- cation	23	89	2	55	54	224
Total	366	1 243	11	265	1 180	3 134

Plaintes reçues selon le répondant (suite)

Pour les plaintes reçues entre le 1^{er} avril 2003 et le 31 mars 2004

Commission nationale des libérations conditionnelles	19
Conseil national des recherches du Canada	3
Ombudsman de la Défense nationale et des Forces canadiennes	1
Commission d'appel des pensions	1
Bureau du Conseil privé	5
Commission de la fonction publique Canada	4
Travaux publics et Services gouvernementaux Canada	5
Monnaie royale canadienne	1
Gendarmerie royale du Canada	129
Solliciteur général Canada	8
Statistique Canada	4
Condition féminine Canada	2
Transports Canada	10
Secrétariat du Conseil du Trésor du Canada	5
Anciens combattants Canada	4
Total	3 134

Enquêtes terminées selon le type de plaintes

Pour les plaintes terminées entre le 1^{er} avril 2003 et le 31 mars 2004

Type de plaintes	Nombre
Accès	782
Collecte	539
Correction — annotation	14
Correction — délais	16
Avis de prorogation	30
Frais inexactes	1
Langue	2
Conservation et retrait	15
Délais	1 511
Utilisation et communication	224
Total	3 134

Plaintes reçues selon le répondant

Pour les plaintes reçues entre le 1^{er} avril 2003 et le 31 mars 2004

8	Agriculture et Agroalimentaire Canada
1	Vérificateur général du Canada, Bureau du
1	Banque du Canada
1	Banque de développement du Canada
265	Agence du revenu du Canada
72	Société canadienne des postes
4	Centre canadien des armes à feu
4	Agence canadienne d'inspection des aliments
1	Patrimoine canadien
2	Commission canadienne des droits de la personne
4	Musée canadien des civilisations
3	Conseil de la radiodiffusion et des télécommunications canadiennes
20	Service canadien du renseignement de sécurité
4	Agence spatiale canadienne
4	Commission canadienne du tourisme
132	Citoyenneté et Immigration Canada
1	Commissariat aux langues officielles
5	Enquêteur correctionnel Canada, Bureau de l'
2 760	Service correctionnel Canada
1	EDULINX Canada Corporation
1	Environnement Canada
1	Finances Canada, ministère des
1	Centre d'analyse des opérations et déclarations financières du Canada
5	Pêches et Océans
22	Affaires étrangères et Commerce international Canada
485	Santé Canada
65	Développement des ressources humaines Canada
15	Commission de l'immigration et du statut de réfugié
2	Affaires indiennes et du Nord Canada
2	Industrie Canada
23	Justice Canada, ministère de la
5	Commission d'examen des plaintes concernant la police militaire
4	Archives nationales du Canada
80	Défense nationale
1	Musée des beaux-arts du Canada

Les dix premiers ministères selon le nombre de plaintes reçues

Pour l'exercice se terminant le 31 mars 2004

Organisation	Total	Accès aux renseignements personnels	Nombre de fois	Atteinte à la vie privée	Autres
Service correctionnel Canada	2 760	1 235	1 335	190	
Santé Canada	485	2	3	480	
Agence des douanes et du revenu du Canada	255	103	72	80	
Citoyenneté et Immigration Canada	132	48	75	9	
Gendarmerie royale du Canada	129	78	34	17	
Défense nationale	80	32	17	31	
Société canadienne des postes	72	13	24	35	
Développement des ressources humaines Canada	65	21	10	34	
Justice Canada	23	8	10	5	
Affaires étrangères et Commerce international	22	4	10	8	
Autres	183	91	39	53	
Total	4 206	1 635	1 629	942	0

Plaintes reçues selon le type de plaintes

Pour les plaintes reçues entre le 1^{er} avril 2003 et le 31 mars 2004

Type de plainte	Nombre
Accès	1 612
Collecte	535
Correction — annotation	20
Correction — délais	27
Avis de prorogation	28
Frais inexacts	1
Langue	2
Conservation et retrait	17
Délais	1 574
Utilisation et communication	390
Total	4 206

Le ministère de la Défense nationale a transmis neuf avis dont sept portaient sur le partage de renseignements avec les membres de la famille après le décès d'un membre des Forces canadiennes.

Les autres avis ont été envoyés par Transports Canada, Travaux publics et Services gouvernementaux Canada, Agriculture et Agroalimentaire Canada, Santé Canada, Affaires indiennes et du Nord Canada, la Commission de l'immigration et du statut de réfugié, le Secrétaire du Conseil du Trésor, Solliciteur général Canada, le Bureau du vérificateur général du Canada, la Commission de la fonction publique du Canada, l'Ombudsman de la Défense nationale et des Forces canadiennes, la Commission des plaintes du public contre la GRC, le SCRS et la Commission nationale des libérations conditionnelles.

Demandes de renseignements

Le Commissariat a donné suite à des milliers de demandes de renseignements du grand public qui voulait obtenir des conseils et de l'aide concernant un vaste éventail de questions liées à la vie privée dans le cadre de transactions avec des institutions fédérales. La demande de renseignements la plus usuelle transmise à notre Commissariat au cours de l'exercice 2003-2004 au sujet de la *Loi sur la protection des renseignements personnels* concernait l'accès aux renseignements personnels détenus par un ministère fédéral. Ces demandes ont été formulées tant par les fonctionnaires fédéraux que par les particuliers. D'autres demandeurs s'inquiétaient en outre du degré de protection des renseignements personnels assuré par certains ministères fédéraux.

Statistiques sur les demandes de renseignements

(du 1^{er} avril 2003 au 30 mars 2004)

Demandes de renseignements téléphoniques reçues	2 580
Demandes de renseignements écrites reçues (courriel, courriel et télécopieur)	2 148
Nombre total de demandes de renseignements reçues	4 728

Communication dans l'intérêt public aux termes de la Loi sur la protection des renseignements personnels

Par la suite, 16 personnes ont déposé des plaintes officielles auprès du Commissariat alléguant que l'ARCC n'avait pas bien protégé leurs renseignements. L'ARCC a reconnu que les procédures de sécurité n'avaient pas été respectées et que l'ordinateur n'avait pas été remis dans une pièce protégée à la fin de la journée. Des mesures disciplinaires conformes à la politique de l'ARCC ont été prises.

L'alinéa 8(2)m) de la *Loi sur la protection des renseignements personnels* confère aux responsables des institutions gouvernementales le pouvoir de communiquer, à leur discrétion, des renseignements personnels d'une personne sans son consentement si la communication peut donner à la personne concernée un avantage ou dans les cas où un intérêt public clairement prédominant l'emporte sur le droit à la vie privée de la personne. Aux termes du paragraphe 8(5), le responsable de l'institution fédérale concernée est tenu d'informer le Commissaire à la protection de la vie privée de la communication des renseignements personnels, de préférence au préalable, à moins qu'une situation d'urgence ne dicte le contraire.

L'année dernière, nous avons reçu 67 avis de ce genre. Service correctionnel Canada (SCC) figurait au premier rang des ministères ayant envoyé des avis. Il en a transmis 20, dont la plupart avaient trait à la communication de renseignements personnels concernant des détenus décédés. SCC recourt souvent aux dispositions de la *Loi sur la protection des renseignements personnels* concernant les communications dans l'intérêt public pour partager des renseignements avec les membres de la famille qui veulent avoir accès aux rapports établis par les employés de SCC qui ont examiné les circonstances entourant le décès d'un détenu.

La GRC a fait parvenir 15 avis de communications imminentes dans l'intérêt public. Ils avaient presque tous trait à des détenus libérés à la fin de leur peine d'emprisonnement que l'on présumait présenter des risques élevés de récidive. La GRC prévoyait recourir à des communications de presse envoyées dans les collectivités où le contrevenant comptait vivre afin d'alerter les résidents de sa présence et des conditions précises associées à sa libération. À titre d'exemple, une de ces conditions pourrait être que le contrevenant ne puisse se rendre sur des terrains d'école, dans des parcs ou des terrains de jeux ou se trouver en compagnie de mineurs.

des renseignements sur les cartes de crédit et le permis de conduire d'une Québécoise. Dans le deuxième incident, une citoyenne canadienne résidant au Colorado, États-Unis, a reçu par erreur le passeport, la carte verte, le certificat de naissance et le numéro de carte de crédit d'une femme vivant au Wisconsin, aux États-Unis, et cette dernière a reçu les documents de la première. Nous avons établi que les deux incidents étaient le fait d'une erreur humaine. Les passeports ont été établis et postés le même jour avec plusieurs milliers d'autres.

Lorsqu'un nombre aussi élevé d'envois est effectué chaque jour, il arrive que des erreurs surviennent au moment de remplir les enveloppes. Le Bureau des passeports a fait savoir que dans les six mois qui séparent ces deux incidents, il avait traité plus de 500 000 demandes. L'accroissement du volume découlait de procédures de sécurité supplémentaires et de restrictions des voyages imposées à l'échelle internationale à la suite des événements du 11 septembre. Depuis la mise en place en janvier 2004 de procédures d'envoi par la poste améliorées, ni le Bureau des passeports, ni le Commissariat n'a reçu de plaintes concernant le mauvais acheminement de documents relatifs aux passeports.

Le vol d'ordinateurs suscite des préoccupations en matière de vie privée

Dans une autre affaire, six ordinateurs ont été volés du bureau des services fiscaux de l'ARC à Laval au Québec. L'un d'entre eux était utilisé pour mettre à l'essai des applications informatiques. Il était protégé au moyen d'un mot de passe et contenait environ deux millions d'enregistrements provenant de quatre bases de données confidentielles. Ces bases contenaient des renseignements personnels mais pas de renseignements relatifs aux déclarations de revenus. Plus de 120 000 personnes faisant partie de ces bases de données ont dû être informées de ce manquement à la sécurité et ont reçu des conseils sur les mesures à prendre pour réduire les possibilités de vol d'identité, notamment celles énumérées ci-après :

- Examiner et vérifier tous les relevés de transactions des comptes de banque, des cartes de crédits et autres transactions financières.
- Signaler à la Société canadienne des postes tout problème ou retard dans la livraison du courrier.
- Signaler à Ressources humaines et Développement des compétences Canada tout soupçon quant à l'utilisation du numéro d'assurance sociale (NAS).
- Communiquer avec une agence d'évaluation de crédit comme Equifax ou Trans-Union qui sont habituées à aider les particuliers en de pareilles circonstances.

alimentaire pour enfants effectués par le contribuable qui permettraient d'établir les droits de ce dernier. Le contribuable s'est dit satisfait du compromis; le dossier a été clos à titre d'affaire « résolue au cours de l'enquête ».

En ce qui concerne la deuxième affaire, le fonctionnaire de l'ARC a remis en question les coûts élevés des médicaments sur ordonnance que la contribuable devait prendre en raison de son état de santé, coûts qui l'empêchaient de rembourser des montants importants de sa dette. Le fonctionnaire lui a demandé de présenter une note de son médecin traitant qui confirmerait son état de santé afin que l'ARC puisse prendre en compte les frais médicaux dans son évaluation des dépenses mensuelles de la contribuable. La plaignante a accepté nos explications concernant la raison fournie par l'ARC pour justifier une telle demande et les répercussions de son refus d'y répondre. Le dossier a été clos à titre d'affaire « résolue au cours de l'enquête ».

Incidents visés par la Loi sur la protection des renseignements personnels

Il arrive qu'on attire notre attention sur des incidents de mauvaise gestion de renseignements personnels pour lesquels un examen plus poussé du Commissariat s'impose. L'an dernier, nous avons effectué 30 examens de ce genre. Il convient de signaler que dans sept de ces incidents, des ministères avaient envoyé par erreur à un client des renseignements personnels concernant d'autres clients.

Cartes d'identification santé envoyées à la mauvaise adresse

Dans une de ces affaires, Anciens combattants Canada (ACC) procédait à la rémission d'environ 143 000 cartes d'identification santé portant le nouveau numéro de téléphone sans frais d'interv bain du Centre d'appels national. Lors de la production de ces cartes, un fichier de données corrompu portant sur environ 12 000 clients en Ontario contenait également les adresses d'autres clients. Avant que l'erreur ne soit constatée, les nouvelles cartes d'identification avaient été envoyées aux mauvaises adresses. Des représentants d'ACC nous ont informés que dès qu'ils ont eu vent du problème, ils ont immédiatement cessé la production et ne l'ont reprise qu'après la mise en place de procédures améliorées de contrôle de qualité. Le Ministère a communiqué avec tous les clients touchés par cette erreur.

Passeports mal acheminés

Le Commissariat s'est également penché sur deux incidents de passeports mal acheminés. Dans un des incidents, un Albertain a reçu, en plus de ses propres documents, une enveloppe du Bureau des passeports contenant le passeport, le certificat de naissance,

Les contribuables doivent se conformer aux demandes de renseignements présentées par l'Agence du revenu du Canada

Aperçu — Première affaire

L'an dernier, le Commissariat a enquêté sur deux affaires qui illustrent le pouvoir conféré à l'Agence du revenu du Canada (ARC) d'exiger des contribuables qu'ils fournissent des renseignements très personnels.

Dans la première affaire, l'ARC a demandé à un Ontarien, lors de la vérification de routine de sa déclaration de revenus de 2001, de fournir copie de l'accord de séparation d'avec son ex-conjointe pour étayer les montants déduits au titre de la pension alimentaire pour enfants. Le contribuable s'est conformé à la demande de l'ARC en lui remettant les parties de l'entente traitant expressément des versements, mais il s'est opposé au fait que l'ARC ait insisté pour obtenir une copie non altérée de l'entente.

Aperçu — Deuxième affaire

Dans la deuxième affaire, une Québécoise s'est plainte des questions détaillées que lui a posées un fonctionnaire de l'ARC qui tentait de recouvrer des montants d'impôt en souffrance. Comme il lui avait été impossible de payer le montant intégral de l'impôt exigible dans un délai raisonnable, elle avait demandé un délai supplémentaire de paiement.

Mesures prises par le CPVP

Après avoir enquêté sur la première affaire, nous avons expliqué au plaignant que la *Loi de l'impôt sur le revenu* conférait à l'ARC le pouvoir juridique d'exiger ces renseignements afin qu'elle puisse se convaincre de l'absence d'autres dispositions de l'entente concernant la pension alimentaire pour enfants susceptibles d'influer sur sa situation fiscale.

En ce qui concerne la deuxième affaire, nous avons établi qu'en pareilles circonstances, l'ARC tentera d'établir un calendrier de remboursement fondé sur la situation financière du débiteur que les deux parties jugent acceptable. Pour ce faire, le débiteur doit communiquer le montant intégral de son revenu et de ses dépenses mensuelles, ce qui comprend ses actifs et ses passifs. Dans l'impossibilité d'arriver à une entente acceptable, l'ARC peut entamer des mesures juridiques de recouvrement de la dette, ce qui comprend la saisie et la vente des actifs du débiteur.

Résultats des mesures prises par le CPVP

Dans la première affaire, afin de limiter l'atteinte à la vie privée, l'ARC a accepté de verser à ses dossiers les seules parties de l'entente se rapportant aux versements de la pension

Correspondance au CRTC affichée sur le site Web

Apéryn

Une personne a écrit au Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) pour signifier son appui concernant la demande de permis adressée par un radiodiffuseur culturel.

Le CRTC a affiché sa correspondance sur son site Web telle qu'il l'a reçue, avec ses nom, adresse, numéro de téléphone et adresse de courriel. Cette pratique est expliquée sur le site Web, mais la personne ne l'avait pas remarquée et ne pensait jamais que sa correspondance serait affichée de cette façon. Elle ne savait pas qu'elle pouvait demander au CRTC de supprimer tout identificateur personnel avant que sa correspondance ne soit affichée.

Lorsqu'elle a appris que ses renseignements personnels étaient affichés sur le site Web, elle en a immédiatement demandé le retrait. Le CRTC s'est conformé à sa demande dans les 48 heures. Entre-temps, toutefois, le moteur de recherche Google (et d'autres peut-être) avait saisi ces renseignements, de sorte que chaque fois que le nom de la personne faisait l'objet d'une recherche au moyen du moteur Google, sa correspondance originale avec le CRTC s'affichait.

La personne a communiqué avec Google pour lui demander de supprimer ses renseignements personnels, mais les représentants de cette entreprise lui ont répondu qu'ils ne le feraient qu'après avoir reçu une demande formelle du webmestre du site ayant affiché pour la première fois les renseignements sur Internet. Elle a fait acheter sa correspondance au CRTC pour que des mesures de suivi adéquates soient prises mais ses renseignements personnels continuaient d'être affichés sur Internet.

Mesures prises par le CPVP

À la suite de l'intervention du Commissariat, le webmestre du CRTC a adressé trois demandes à Google, mais aucune d'entre elles n'a fait l'objet d'une réponse officielle. Google a néanmoins fini par supprimer les renseignements personnels de la personne, au soulagement et à la satisfaction de cette dernière.

Résultats des mesures prises par le CPVP

Nous avons clos le dossier à titre d'affaire « résolue au cours de l'enquête ».

contact de l'équipage du navire. Tous les autres renseignements recueillis portent sur les activités de pêche sous observation.

Si, par nature, la présence d'un étranger à bord des navires est envahissante, la question relève de la vie privée « personnelle », laquelle n'est pas assujétie à la *Loi sur la protection des renseignements personnels*, et non de la protection des renseignements personnels.

Résultats des mesures prises par le CPVP

Le Commissariat a conclu que les plaintes étaient non fondées. Malgré cette conclusion, nous avons discuté des préoccupations des plaignants avec des représentants de Pêches et Océans Canada, qui ont soutenu que le Ministère doit pouvoir continuer à surveiller les activités de pêche. Ils ont toutefois convenu de consulter l'industrie de la pêche et nous les avons encouragés à recommander des solutions moins envahissantes pour exécuter les activités de ce programme.

TRAITEMENT DES RENSEIGNEMENTS PERSONNELS

Où êtes-vous né?

Apéryn

Une personne s'est plainte de la pratique du ministère des Affaires étrangères et du Commerce international qui consiste à afficher le lieu de naissance sur le passeport du détenteur, pratique qui, à son avis, est discriminatoire et porte atteinte à la vie privée.

Mesures prises par le CPVP

Il est ressorti de notre enquête que plus de 85 pays exigent l'inscription du lieu de naissance sur le passeport à titre de condition d'admission au pays. Des fonctionnaires du ministère des Affaires étrangères ont fait savoir que, lors des négociations des ententes de dispense réciproque de visas, le lieu de naissance figure souvent parmi les conditions imposées par d'autres pays. Pour sa part, l'Organisation de l'aviation civile internationale recommande elle aussi l'inclusion du lieu de naissance sur les documents de voyage.

Quoi qu'il en soit, depuis 1986, les détenteurs de passeport ont le choix de faire ou non inscrire ce renseignement. Ceux qui optent pour l'exclusion de ce renseignement doivent signer des attestations stipulant qu'ils ont été informés des éventuelles difficultés qu'ils pourraient rencontrer à certains postes frontaliers, comme le fait que des douaniers leur posent des questions supplémentaires, la nécessité d'obtenir un visa ou même le refus d'entrée.

Résultats des mesures prises par le CPVP

Nous avons conclu que la plainte était non fondée.

Il est ressorti de l'enquête que le Programme des observateurs est autorisé par règlement. Les fonctions des observateurs consistent à surveiller les activités de pêche, notamment en examinant et en mesurant les gréments, en vérifiant le poids et les espèces des poissons pêchés, en inspectant les dossiers des pêches et en effectuant un échantillonnage biologique des poissons. Les seuls renseignements personnels que les observateurs recueillent dans le cours normal de leurs fonctions sont les noms, adresses et numéros de

Mesures prises par le CPVP

Le Commissariat a reçu deux plaintes concernant le Programme canadien des observateurs de Pêches et Océans Canada qui exige des pêcheurs, comme condition d'obtention de leur permis, qu'ils permettent à un observateur de les accompagner à bord de leurs navires de pêche commerciale, et ce, même le soir, pendant la nuit et en dehors des heures de pêche. Certains pêcheurs n'accueillent que des membres de leur famille sur leurs navires; ceux-ci n'étant pas assez grands pour recevoir un étranger. Une des plaintes portait également sur le caractère envahissant d'une solution de rechange à la présence d'un observateur à bord de leur navire, soit la surveillance électronique au moyen de caméras vidéo et de systèmes mondiaux de localisation.

Appercu

Une expédition de pêche pas comme les autres?

L'enquête a permis à l'autorité portuaire de mettre en place des mesures de sécurité qui veillent à ce que les données recueillies par les caméras soient bien protégées, qu'elles ne soient pas conservées plus longtemps que nécessaire et que l'accès aux renseignements et la communication de ceux-ci soient strictement limités. Compte tenu de la volonté de l'autorité portuaire de donner suite à nos préoccupations, l'affaire est considérée résolue.

Les représentants de l'autorité portuaire ont volontiers accepté de retirer les caméras qui surveillaient ce secteur et d'apposer des affiches informant le public de la présence de caméras de surveillance sur le port.

Résultats des mesures prises par le CPVP

Nous ne nous opposons pas à ce que des caméras soient installées dans presque tous ces secteurs à des fins de sécurité. Toutefois, nous nous inquiétons de la surveillance des activités sur le trottoir accessible au public.

Mesures prises par le CPVP

où les pêcheurs et d'autres propriétaires de navires jettent les substances polluantes de leurs navires qui pourraient nuire à l'environnement).

Mesures prises par le CPVP

Nous avons établi que la femme devait se soumettre au même processus de sélection qu'un candidat à un poste d'agent de police. La GRC n'a cependant pas été en mesure de démontrer la pertinence de ces questions pour un poste civil de bureau. Nous avons conclu que la plainte était fondée.

Résultats des mesures prises par le CPVP

À la suite des discussions avec la GRC, les représentants de ses services de santé ont accepté de cesser d'utiliser ce questionnaire pour les candidats civils. La GRC a entrepris la rédaction d'un nouveau formulaire réservé aux candidats à des postes d'agents des télécommunications qui comportent des exigences médicales liées au poste, comme l'ouïe, les mouvements du torse et les maladies susceptibles de toucher les capacités de réflexion cognitive et de reconnaissance de la parole.

Bien que la femme se soit aussi opposée à l'obligation de subir une évaluation psychologique, la GRC a expliqué que les agents des télécommunications représentent souvent la seule ligne de vie entre les victimes et les agents qui interviennent dans une situation d'urgence, explication que nous avons jugée satisfaisante. La GRC doit donc s'assurer que les candidats sont en mesure de soutenir la pression associée au travail et qu'ils puissent aisément composer avec les situations qu'ils rencontrent. La collecte de renseignements personnels visant à évaluer la capacité des candidats à gérer ces stress est par conséquent raisonnable et appropriée.

TECHNOLOGIES DE SURVEILLANCE**Réduction du nombre de caméras de surveillance vidéo au port de Nanaimo****Aperçu**

Un résident de la Colombie-Britannique, conscient de la position de l'ancien commissaire concernant la surveillance vidéo dans les rues de Kelowna, a déposé une plainte au sujet des projets de l'autorité portuaire de Nanaimo d'installer des caméras de surveillance vidéo dans le port.

Entre autres choses, l'autorité portuaire fournit des installations de mouillage et les clients qui paient pour ce service s'attendent à ce qu'elle protège leurs biens. Après avoir reçu plusieurs plaintes de clients concernant du vandalisme et des vols sur les navires, l'autorité portuaire a songé à installer des caméras sur ses quais et envisage de le faire ailleurs (bureaux de l'autorité portuaire, terrains de stationnement, trottoir, buanderies et l'endroit

Les candidats devaient en outre dire s'ils avaient des varices, de l'arthrite, des phlébites, le rhume des foies, une maladie vénérienne et préciser si des membres de leur famille avaient le diabète, le cancer, la tuberculose, une maladie cardiaque ou faisaient de l'hypertension.

- « Avez-vous des menstruations tous les mois? »
- « Quelle est la date de vos dernières menstruations? »
- « Vos menstruations sont-elles douloureuses? »
- « À quand remonte votre dernier test Pap? »
- « Combien de fois avez-vous été enceinte, en comptant les avortements et les fausses couches? »

On a refusé à une femme le poste d'agent civil des communications à la GRC parce qu'elle avait refusé de répondre à certaines questions d'un questionnaire sur les antécédentes médicales qu'elle devait remplir dans le cadre du processus de recrutement. Voici quelques-unes de ces questions :

Apéryn

Questionnaire médical de la GRC jugé trop indiscret pour les candidats civils

Le Commissariat a offert en permanence son soutien afin d'arriver à un juste équilibre entre les intérêts en matière de vie privée des bénéficiaires et les impératifs du programme de Santé Canada.

- Le Ministère élabore un Code de la protection des renseignements personnels qui énonce les pratiques du Ministère en matière de collecte, d'utilisation et de communication. Le Code respecte la norme supérieure de consentement de la Loi sur la protection des renseignements personnels et les documents électroniques, puisque nombre des tiers fournisseurs de services associés au programme de Santé Canada sont assujettis à cette loi.
- Le Ministère a mis sur pied le comité d'examen de la consommation pharmaceutique de Santé Canada et des Premières Nations, composé de professionnels de la santé agréés, d'experts en évaluation de l'utilisation des médicaments, en de santé des Autochtones et en utilisation des médicaments;
- Le Ministère instaure un mécanisme d'obtention du consentement des bénéficiaires par le biais de questions liées à la sécurité des patients ou de préoccupations quant à l'utilisation à mauvais escient du programme;
- Le Ministère élabore un Code de la protection des renseignements personnels qui énonce les pratiques du Ministère en matière de collecte, d'utilisation et de communication. Le Code respecte la norme supérieure de consentement de la Loi sur la protection des renseignements personnels et les documents électroniques, puisque nombre des tiers fournisseurs de services associés au programme de Santé Canada sont assujettis à cette loi.

Plusieurs associations autochtones, notamment l'Assemblée des Premières Nations et les Inuits Tapiriit Kanatami, ont appuyé les plaintes et présenté des arguments au nom de leurs membres. Cette campagne a été initiée suite à la recommandation de la vérificatrice générale qui demandait à Santé Canada d'améliorer ses mécanismes de suivi pour éviter l'abus des médicaments prescrits. Santé Canada s'est également efforcé de respecter le droit des bénéficiaires d'être informés de toutes les conséquences éventuelles d'un examen de l'utilisation de ces médicaments.

Les plaignants estimaient que les droits aux prestations du programme étaient et avaient toujours été prévus dans les traités et qu'ils ne pouvaient faire autrement que de convenir des pratiques d'examen que Santé Canada prévoyait imposer sans quoi ils perdraient leurs prestations. Ils se sont opposés au libellé compliqué du formulaire, à sa vaste portée et au manque de mesures satisfaisantes de protection des renseignements personnels détenus par des tiers fournisseurs de services.

Mesures prises par le CPVP

Nous avons accepté les plaintes conformément aux dispositions de la *Loi sur la protection des renseignements personnels*, puis déterminé qu'aucune disposition de cette loi n'avait été enfreinte. Le Commissariat a cependant continué de collaborer avec les associations autochtones et le Ministère afin d'arriver à une nouvelle manière de présenter l'initiative relative au consentement qui traite des préoccupations concernant la vie privée. Ensemble, nous avons identifié les points essentiels du programme de prestations de santé exigeant le consentement éclairé des bénéficiaires. Nous avons par ailleurs reconnu que les dispositions relatives à la protection des renseignements personnels des contrats conclus avec les tiers fournisseurs de services devaient être renforcées, ce que Santé Canada s'est engagé à faire. Enfin, nous nous sommes entendus sur la nécessité de rédiger les formulaires de consentement en des termes les plus simples et les plus clairs possible.

Résultats des mesures prises par le CPVP

Santé Canada a par la suite proposé une autre démarche relative au formulaire de consentement que les intervenants autochtones ont soutenue. Il s'agit de la démarche suivante :

- le Ministère continuera de promouvoir l'obtention du consentement à titre de pratique exemplaire (position qui reçoit l'aval du Commissariat), mais n'exigera plus que tous signent le formulaire;

Résolue au cours de l'enquête : le Commissariat a aidé à négocier une solution qui satisfait toutes les parties dans le cadre de l'enquête. Aucune conclusion n'est rendue.

Abandonnée : l'enquête a pris fin avant que toutes les allégations soient pleinement examinées. Une affaire peut être *abandonnée* pour toutes sortes de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, lesquels sont essentiels pour arriver à une conclusion.

Résolue hâtivement : le Commissariat a commencé à utiliser cette nouvelle disposition en avril 2004 pour traiter des situations où l'affaire est réglée avant même qu'une enquête officielle ne soit entamée. À titre d'exemple, si le sujet de la plainte déposée par une personne a déjà fait l'objet d'une enquête par le Commissariat et a été jugé conforme à la *Loi sur la protection des renseignements personnels*, nous lui expliquerions la situation. Nous avons en outre reçu des plaintes qui, si elles faisaient l'objet d'une enquête formelle, pourraient avoir des retombées négatives sur la personne. En pareil cas, nous expliquerions en profondeur la situation aux plaignants. S'ils décident alors de ne pas poursuivre l'affaire, celle-ci est alors « *résolue hâtivement* ».

Cas choisis en vertu de la Loi sur la protection des renseignements personnels

SOINS DE SANTÉ

Programme de prestations de santé non assurées de Santé Canada

À l'écart

À l'été 2003, le CPVP a reçu plusieurs centaines de plaintes et de nombreuses demandes de renseignements concernant la décision de Santé Canada d'exiger des bénéficiaires des Premières Nations et Inuits de certaines prestations de santé subventionnées par le gouvernement qu'ils signent un formulaire de consentement avalisant les pratiques du Ministère en matière de collecte, d'utilisation et de communication de leurs renseignements personnels. Les plaignants se sont opposés au libellé compliqué du formulaire, à sa vaste portée et au manque de mesures satisfaisantes de protection des renseignements personnels détenus par des tiers fournisseurs de services.

Par ailleurs, la productivité a atteint un sommet record cette année, le nombre de plaintes résolues par les enquêteurs s'établissant à 3 315.

Plaintes en vertu de la loi sur la protection des renseignements personnels

La productivité des enquêteurs a été à son plus fort cette année (3 134 plaintes ayant été résolues). Toutefois, bien que nous ayons résolu 3 483 affaires cette année, 2 323 d'entre elles représentaient des enquêtes qui avaient été menées deux ans auparavant. Les statistiques pour cette année représentent les enquêtes actives achevées en 2003-2004. Les conclusions relatives à ces plaintes ont été rendues comme suit :

Non fondées	1 243
Fondées	1 180
Fondées et résolues	69
Résolues	11
Résolues au cours de l'enquête	265
Abandonnées	366

Définitions des conclusions aux termes de la loi sur la protection des renseignements personnels

Non fondée : l'enquête n'a pas permis de déceler des éléments de preuve qui suffisent à conclure que l'institution fédérale n'a pas respecté les droits d'un plaignant aux termes de la Loi sur la protection des renseignements personnels.

Fondée : l'institution fédérale n'a pas respecté les droits d'une personne aux termes de la Loi sur la protection des renseignements personnels.

Fondée et résolue : les allégations sont corroborées par l'enquête et l'institution fédérale a accepté de prendre des mesures correctives pour remédier à la situation.

Résolue : cette conclusion est réservée aux plaintes pour lesquelles une conclusion *fondée* serait trop sévère pour qualifier une situation relevant essentiellement d'une mauvaise communication ou d'un malentendu. Elle signifie que le Commissariat, après avoir mené une enquête complète et minutieuse, a permis de négocier une solution qui satisfait toutes les parties.

La Commissaire est tenue de déposer un rapport annuel au Parlement sur les activités du Commissariat au cours de l'exercice précédent. Le présent rapport vise la période comprise entre le 1^{er} avril 2003 et le 31 mars 2004 au titre de la *Loi sur la protection des renseignements personnels*.

ENQUÊTES ET DEMANDES DE RENSEIGNEMENTS

Le Commissariat à la protection de la vie privée est chargé de mener des enquêtes sur les plaintes que déposent des personnes aux termes de l'article 29 de la *Loi sur la protection des renseignements personnels* (et de l'article 11 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, connue sous l'acronyme *LPDPDE*).

Ces enquêtes permettent de déterminer si les droits à la vie privée des personnes ont été enfreints et si ces dernières ont pu avoir accès à leurs renseignements personnels. Lorsque les droits à la vie privée et le droit d'accès ont été enfreints, le processus d'enquête cherche à trouver des voies de recours pour les personnes et à empêcher que les violations ne se reproduisent. L'an dernier, le Commissariat a reçu 4 206 nouvelles plaintes, un record inégalé représentant une hausse de 250 pour 100 par rapport à l'année précédente. Plusieurs facteurs ont contribué à cet état de chose :

- 472 membres des collectivités autochtones du Canada se sont plaints d'avoir été tenus par Santé Canada de signer un formulaire de consentement rédigé en termes très généraux pour recevoir des prestations de santé subventionnées par le gouvernement;
- 608 agents de correction ont déposé plus de 1 100 plaintes contre Service correctionnel Canada (SCC) alléguant que le Ministère avait refusé de leur fournir des copies de leurs dossiers personnels;
- 107 employés de l'établissement de Joyceville ont déposé une plainte contre SCC alléguant que le Ministère avait omis de protéger leurs renseignements personnels lorsqu'une liste des adresses et numéros à domicile des employés a été trouvée parmi la population carcérale;

- 38 contrevenants de la Colombie-Britannique ont déposé au total 950 plaintes contre SCC alléguant que le Ministère n'avait pas répondu en temps opportun à leurs demandes d'accès à leurs renseignements personnels versés à 25 fichiers de renseignements personnels standard que SCC tient sur les contrevenants.

Rapport concernant la Loi sur la protection des renseignements personnels

INTRODUCTION

La Loi sur la protection des renseignements personnels, en vigueur au Canada depuis 1983, protège les renseignements personnels concernant les personnes que détiennent des institutions du gouvernement fédéral. La Loi régit la manière dont les ministères et organismes fédéraux recueillent, utilisent, communiquent, conservent et détruisent des renseignements personnels. Elle confère aux personnes le droit de demander accès à leurs renseignements personnels détenus par le gouvernement et celui de demander que des corrections y soient apportées. De plus, elle établit les fonctions, les responsabilités et le mandat du Commissaire à la protection de la vie privée du Canada.

La Commissaire reçoit des plaintes de personnes estimant que leurs droits en vertu de la Loi sur la protection des renseignements personnels ont été enfreints et mène des enquêtes sur ces plaintes. Elle peut également déposer une plainte et mener une enquête de sa propre initiative si elle estime qu'il existe des motifs raisonnables de croire que la Loi a été enfreinte.

La Commissaire à la protection de la vie privée du Canada agit à titre d'ombudsman afin de résoudre autant que possible les plaintes grâce à la médiation, la négociation et la persuasion.

Toutefois, la Loi confère à la Commissaire de vastes pouvoirs d'enquête lui permettant d'acquiescer de son mandat. Elle peut assigner des témoins à comparaître et à témoigner, pénétrer dans des locaux pour se faire remettre des documents et mener des entrevues. L'enquête aux enquêtes constitue une infraction à la Loi. La Loi ne confère pas à la Commissaire le pouvoir de rendre des ordonnances.

Toutefois, la Commissaire peut recommander au besoin des changements des pratiques de traitement des renseignements menées par les institutions gouvernementales, prérogative qu'elle exerce de fait. Par ailleurs, elle peut mener en tout temps des vérifications auprès de ministères ou d'organismes fédéraux et recommander que soient modifiées les pratiques qui ne sont pas conformes à la Loi sur la protection des renseignements personnels.

plus vaste. Contrairement à la *LPRPDE*, ces lois s'appliquent à toutes les organisations, à quelques exceptions près, et non seulement à celles qui exercent des activités commerciales. De plus, contrairement à la *LPRPDE*, elles contiennent des règles régissant les renseignements personnels des employés qui diffèrent de celles visant les autres renseignements personnels. En outre, elles confèrent aux deux commissaires provinciaux le pouvoir de rendre des ordonnances, par exemple, pour exiger d'une organisation qu'elle donne à une personne accès aux renseignements personnels à son sujet ou pour exiger d'une organisation qu'elle cesse de recueillir, d'utiliser ou de communiquer certains de ces renseignements personnels. À titre comparatif, le Commissaire à la protection de la vie privée du Canada ne jouit pas du pouvoir de rendre des ordonnances.

En nous fondant sur les critères établis dans cet avis, soit la présence des dix principes de l'annexe 1 de la *LPRPDE*, les examens et recours indépendants et une disposition limitant la collecte, l'utilisation et la communication des renseignements aux seules fins légitimes (le critère de la personne raisonnable), nous avons conclu que, dans l'ensemble, les lois de la Colombie-Britannique et de l'Alberta sont essentiellement similaires à la *LPRPDE*.

Une autre initiative législative mérite d'être signalée, à savoir le dépôt et l'adoption du projet de loi 31 de l'Ontario, la *Loi sur la protection des renseignements sur la santé*. La loi a reçu la sanction royale le 20 mai 2004 et devrait entrer en vigueur le 1^{er} novembre 2004. Nous poursuivons toujours notre examen de cette loi et ne sommes pas encore en mesure d'affirmer si elle est ou non réputée essentiellement similaire à la *LPRPDE*.

Le ministre a déclaré qu'il sollicitera le point de vue du Commissariat à la protection de la vie privée afin de déterminer si la législation est essentiellement similaire et il inclura le point de vue de ce dernier dans la soumission au gouverneur en conseil. Le processus offre également une occasion au public et aux parties intéressées de commenter la législation dont il est question.

Selon l'avis publié dans la *Gazette du Canada*, le ministre s'attend à ce que les lois essentiellement similaires des provinces ou des territoires comportent les éléments suivants :

- elles intègrent les dix principes de l'annexe 1 de la *LPRPDE*;
- elles prévoient un mécanisme de surveillance et de recours indépendant et efficace comportant des pouvoirs d'enquête;
- elles restreignent la collecte, l'utilisation et la communication des renseignements personnels à des fins appropriées ou légitimes.

Lois provinciales et territoriales adoptées à ce jour

Conformément au paragraphe 25(1) de la *LPRPDE*, le Commissariat à la protection de la vie privée est tenu de rendre compte chaque année au Parlement de la « mesure dans laquelle les provinces ont édicté des lois essentiellement similaires » à la *Loi*.

La *Loi sur la protection des renseignements personnels dans le secteur privé* de la province de Québec est entrée en vigueur, avec quelques exceptions, le 1^{er} janvier 1994. Elle contient des dispositions détaillées qui augmentent les droits à la protection des renseignements des articles 35 à 41 du *Code civil du Québec* et leur donnent force de loi. En novembre 2003, la gouverneure générale a pris un décret (C.P. 2003-1842, 19 novembre 2003) qui exclut certaines organisations de cette province, autres que des ouvrages, entreprises et secteurs d'activités fédéraux, du champ d'application de la *LPRPDE*.

Au printemps 2003, les provinces de la Colombie-Britannique et de l'Alberta ont déposé des textes de loi similaires, soit respectivement le projet de loi 38 et le projet de loi 44. Les deux projets de loi ont été adoptés par les assemblées législatives et sont entrés en vigueur le 1^{er} janvier 2004.

Les deux lois, qui portent le même titre, soit *Personal Information Protection Act*, sont similaires à la *LPRPDE* sans toutefois y être identiques, leur champ d'application étant

LOIS PROVINCIALES ESSENTIELLEMENT SIMILAIRES

Aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), le gouverneur en conseil peut prendre un décret excluant une organisation, une catégorie d'organisations, une activité ou une catégorie d'activités de l'application de la LPRPDE à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels, lequel s'effectue à l'intérieur d'une province ayant adopté une loi réputée essentiellement similaire à la LPRPDE.

Le but de cette disposition est de permettre aux provinces et territoires de réglementer les pratiques de gestion des renseignements personnels des organisations faisant affaire à l'intérieur de leurs frontières, sous réserve qu'ils disposent d'une loi qui soit essentiellement similaire à la LPRPDE.

S'il y a décret, la LPRPDE ne s'applique pas à la collecte, à l'utilisation ou à la communication de renseignements personnels par des organisations assujetties à la loi provinciale. Néanmoins, les renseignements personnels, communiqués à l'extérieur de cette province ou du pays continueront d'être assujettis à la LPRPDE, laquelle contiendra également de s'appliquer, dans les limites d'une province, aux ouvrages, aux entreprises et aux secteurs d'activités sous réglementation fédérale, ce qui comprend les banques, les compagnies aériennes, les radiodiffuseurs et les entreprises de télécommunications.

Processus d'évaluation des lois provinciales et territoriales

Le 22 septembre 2001, Industrie Canada a publié un avis établissant le processus que le Ministère utilisera pour déterminer si les lois provinciales ou territoriales sont réputées être essentiellement similaires.

Le processus sera enclenché lorsqu'une province, un territoire ou une organisation informera le ministre de l'Industrie d'une loi qui, à son avis, est essentiellement similaire à la LPRPDE. Le ministre peut aussi agir de son propre chef et recommander au gouverneur en conseil de désigner une loi provinciale ou territoriale comme étant essentiellement similaire.

Position du CPVP

La disposition de la *LPRPDE* relative au caractère « essentiellement similaire » des lois assure des niveaux uniformes de protection de la vie privée dans tous les secteurs de l'économie du pays, mais elle ne régle pas tous les problèmes comme par magie. La protection harmonisée de la vie privée présente en soi des défis bien particuliers.

Conscients de ces défis, la Commissaire fédérale et ses homologues provinciaux/territoriaux à la protection de la vie privée et les membres de leurs effectifs ont concerté leurs efforts pour mieux faire comprendre aux entreprises à quelles lois elles sont assujetties et pour aider les particuliers à comprendre leurs droits et les recours mis à leur disposition dans les lois qui s'y rapportent. Les commissaires à l'information et à la protection de la vie privée de la Colombie-Britannique et de l'Alberta ont publié conjointement un guide (disponible sur leurs sites Web et à partir d'un lien sur notre site) qui aide les entreprises et les particuliers à démêler une situation qui, initialement, paraît déconcertante. Le guide complète les travaux exécutés par le Commissariat afin de publier divers documents comme la diffusion en temps réel d'une allocution prononcée par la Commissaire et une trousse électronique à l'intention des entreprises, le tout dans le but de faciliter la mise en œuvre de la *LPRPDE*.

Dans un monde de plus en plus informatisé et perfectionné sur le plan technologique, chaque jour, voire chaque minute, semble apporter son lot de nouvelles menaces éventuelles à la protection des renseignements personnels. Dans un avenir rapproché, le Commissariat est résolu à favoriser une bonne compréhension des nouveaux enjeux en matière de vie privée auprès des parlementaires, du grand public et des législateurs, de même qu'à continuer de formuler une analyse convaincante des risques et défis nationaux et internationaux en matière de protection de la vie privée à mesure qu'ils se présentent.

Réglementation du droit à la vie privée dans un régime fédéral

chargé de mettre au point des outils de communication et d'élaborer des directives, de répondre aux questions et de rencontrer des associations de soins de santé pour dissiper leurs inquiétudes et expliquer la position du Commissariat.

Nous avons constaté que tous les volets du secteur des soins de santé n'anticipent pas d'importants problèmes de conformité avec la *LPRPD*. À titre d'exemple, le Collège royal des chirurgiens dentistes de l'Ontario a préparé un excellent dossier sur la conformité à la loi qu'il a remis à tous les cabinets de dentistes de l'Ontario.

Dans une économie moderne où les renseignements personnels circulent librement entre les limites territoriales (par exemple, des renseignements concernant des clients à Madrid d'une entreprise dont le siège est à Montréal peuvent être traités à Berlin, puis stockés à Vancouver), la protection de la vie privée se doit d'être homogène et harmonisée. Les particuliers ont besoin que les renseignements personnels les concernant tout autant que leurs droits à cet égard soient protégés, quelle que soit l'administration vers laquelle ils sont acheminés.

Cette tâche est difficile à remplir à l'échelle internationale et exige des négociations et des rajustements en permanence. Même si les renseignements ne quittent jamais le pays, cette tâche pose un défi de taille dans un régime fédéral comme celui du Canada où les responsabilités des secteurs de compétence varient sensiblement. Au cours de l'année visée par l'examen, nombre de faits nouveaux importants sont survenus dans le processus menant vers une protection entière et harmonisée de la vie privée au Canada.

En octobre 2003, le gouvernement de la Colombie-Britannique a adopté la loi dite *Personal Information Protection Act* qui s'applique aux activités commerciales du secteur privé. L'Alberta lui a emboîté le pas, en décembre 2003, lorsqu'elle a adopté une loi essentiellement similaire portant le même titre. Le 1^{er} janvier 2004, la version intégrale de la *LPRPD* est entrée en vigueur, de sorte qu'elle s'applique maintenant à l'ensemble des activités commerciales au Canada sauf dans les provinces ayant adopté des lois provinciales essentiellement similaires à la loi fédérale. En novembre 2003, la gouverneure en conseil a déclaré que la *Loi sur la protection des renseignements personnels dans le secteur privé* de la province de Québec était essentiellement similaire à la loi fédérale. À la mise sous presse du présent rapport, des déclarations semblables étaient attendues pour les lois de la Colombie-Britannique et l'Alberta.

Les cabinets de médecin et ceux d'autres professionnels, tels les dentistes et les chiropraticiens, exercent des activités commerciales. Par conséquent, les renseignements personnels qu'ils recueillent, utilisent et communiquent sont assujettis à la *LPRPDE*. La *Loi* ne s'applique pas aux activités essentielles des hôpitaux, à savoir les soins aux patients. Ce dossier relève manifestement de la compétence des provinces (même si la *LPRPDE* s'appliquerait à des activités périphériques manifestement commerciales comme l'exploitation d'un terrain de stationnement, laquelle exploitation pourrait impliquer la collecte de renseignements personnels).

Position du CPPP

Le Commissariat est d'avis que la *LPRPDE* constitue un moyen très pratique de protéger les renseignements personnels sur la santé sans pour autant imposer un fardeau déraisonnable aux professionnels de la santé. Dans l'ensemble, le rapport traditionnel entre le médecin et son patient ne sera pas appelé à changer considérablement. Le consentement donné par le patient pour la collecte, l'utilisation et la communication des renseignements personnels doit être fondé sur la connaissance de leurs fins. Cela ne suppose pas que les médecins doivent avoir des conversations avec tous leurs patients. Il suffit, pour informer les patients, de recourir à des avis, des affiches, des brochures et des renseignements sur les formulaires que ces derniers remplissent habituellement lorsqu'ils donnent leurs antécédents médicaux.

Par ailleurs, le patient peut raisonnablement s'attendre à ce que les renseignements le concernant soient utilisés ou communiqués de différentes façons et à maintes reprises pour qu'il puisse recevoir des soins et des traitements. C'est notamment le cas des renseignements qu'un omnipraticien communique à un spécialiste ou à un laboratoire ou celui des renseignements que le médecin et le pharmacien échanagent lorsqu'ils discutent d'une ordonnance. En ce qui concerne ces utilisations et communications raisonnablement prévues des renseignements personnels d'un patient, les professionnels de la santé peuvent compter sur un consentement implicite tant qu'il est fondé sur une connaissance générale de la manière dont les renseignements personnels seront utilisés et communiqués. Il serait nécessaire d'obtenir un consentement explicite dans le cas d'utilisations et de communications auxquelles le patient ne s'attendrait pas normalement. La communication de renseignements à des fins de recherche figure parmi les exemples de situations où un tel consentement devrait être obtenu.

Pour aborder ces préoccupations et promouvoir cette façon sensée d'appliquer la *LPRPDE*, le Commissariat a joint ses efforts à ceux de Santé Canada, d'Industrie Canada et de Justice Canada pour former un groupe de travail interministériel

En 2003, divers groupes du secteur des soins de santé ainsi que les ministères de la Santé provinciaux et territoriaux approuvaient de plus en plus l'arrivée imminente de la date butoir de janvier 2004 à partir de laquelle la *LPRPD* s'appliquerait à toutes les activités commerciales. Ils ont de nouveau fait connaître leurs craintes concernant l'incidence de la *Loi* sur le secteur des soins de santé, certaines parties allant même jusqu'à demander officiellement que la *Loi* soit modifiée de manière à retirer les renseignements sur la santé de son champ d'application ou à retarder la prochaine étape prévue de sa mise en œuvre.

L'assujettissement des renseignements personnels sur la santé à la *LPRPD* a troublé plus d'un intervenant du secteur des soins de santé et ce, avant même que la *Loi* ne soit adoptée. C'est donc en partie par souci de dissiper les incertitudes dans ce dossier que le Parlement a choisi de soustraire les renseignements personnels sur la santé du champ d'application de la *Loi* pour l'année suivant son adoption.

Protection des renseignements personnels sur la santé

C'est pour cette raison que l'actuelle Commission a comparu en mars 2004 devant le Comité sénatorial chargé d'examiner ce projet de loi et qu'elle a fait connaître ses craintes. Bien que le Parlement ait décidé d'adopter la loi en dépit de l'opposition du Commissariat et d'autres défenseurs de la vie privée, cette question continue de nous préoccuper tout autant.

L'application de la loi au sens conventionnel du terme.

d'agir à titre d'agents de l'État dans la lutte contre le terrorisme, mais aussi dans forces de l'ordre et aux organismes de sécurité nationale, ce qui, de fait, leur permet consentement de l'intéressé dans le but de les communiquer au gouvernement, aux organisations du secteur privé de recueillir des renseignements personnels sans le cinq ans ou plus. De plus, la *Loi* modifie la *LPRPD* afin qu'elle permette aux pour avoir commis une infraction passible d'une peine d'emprisonnement de nationale, mais aussi toute personne dont le nom figure sur un mandat d'arrestation et les exploitants de systèmes de réservation de services aériens pour identifier non de se servir des renseignements sur les passagers fournis par les transporteurs aériens peu après la fin de la période visée par notre rapport, permet à la GRC et au SCRS La *Loi sur la sécurité publique* de 2002, qui a reçu la sanction royale le 6 mai 2004, soit sur les passagers par des organismes de sécurité continue de se poser.

présenter. Un compromis entre le Commissariat et l'ADRC a permis de régler en partie ce dossier, mais la question plus vaste de l'accès aux renseignements personnels

Accès du gouvernement aux renseignements personnels détenus par les entreprises

Peu de temps après son entrée en fonction, l'actuelle Commissaire a décidé d'améliorer la manière d'aborder cette question et a élaboré des lignes directrices concernant l'utilisation de la surveillance vidéo par les autorités publiques. Ces lignes directrices énoncent les principes d'évaluation de la nécessité de recourir à la surveillance vidéo et, lorsqu'elle est menée, elles garantissent que l'incidence sur la vie privée sera minimale. Par exemple, le recours à la surveillance vidéo devrait donner suite uniquement à un problème réel et urgent lorsque des méthodes moins envahissantes ne sauraient suffire. Les systèmes de surveillance vidéo devraient être conçus de manière à avoir le moins de répercussions possible sur la vie privée. Ils devraient être utilisés pendant des périodes limitées et ne devraient pas capter d'images dans des lieux tels que l'intérieur d'un bureau ou d'un appartement, endroits où les gens s'attendent encore plus à ce que soit protégé leur droit à la vie privée.

Un autre sujet inquiète le Commissariat, les défenseurs de la vie privée et les commissaires à la protection de la vie privée : l'accès par les forces de l'ordre et les organismes de sécurité nationale aux renseignements personnels recueillis par des organisations du secteur privé. Nombre de gens s'opposent à la collecte de renseignements les concernant par le secteur privé parce qu'ils s'inquiètent surtout que ces renseignements puissent, d'une manière ou d'une autre, se retrouver entre les mains du gouvernement.

Cette collecte peut à l'occasion être légitime, mais, sans contrôle ni surveillance, elle peut conférer aux organisations du secteur privé le rôle d'agent d'application de la loi et les forcer à remettre les renseignements personnels qu'elles ont recueillis pour des motifs tout à fait différents, ce qui va à l'encontre des pratiques équitables les plus fondamentales en matière de renseignements.

Position du CPVP

Le Commissariat a réellement commencé à se préoccuper de ce dossier en 2003 lorsque les compagnies aériennes ont été tenues de communiquer des renseignements personnels sur les passagers – notamment leur itinéraire, leurs compagnons de voyage, le mode de paiement des billets, les adresses et numéros de téléphone des contacts et, même, les préférences alimentaires et les besoins de santé – à ce qui était à l'époque l'Agence des douanes et du revenu du Canada, de sorte que les agents des douanes et de l'immigration puissent évaluer les risques à la sécurité que les voyageurs pouvaient

Surveillance vidéo

La surveillance vidéo pourrait bien être l'exemple le mieux connu et le plus évident des technologies de surveillance. Certains ont de la difficulté à s'imaginer, voire à saisir le sentiment que leur « vie privée » est protégée lorsqu'ils se trouvent dans un parc public ou qu'ils se promènent sur une rue de la ville, entourés de gens qui peuvent bien les voir et les entendre. En revanche, rares sont ceux qui n'arrivent pas à juger malsain le fait que des caméras les surveillent et enregistrent peut-être leurs moindres faits et gestes chaque fois qu'ils sortent de chez eux et peu importe où ils se trouvent. Nous ne sommes pas encore rendus à ce stade au Canada, contrairement au Royaume-Uni qui compte environ 4 millions de caméras, soit une caméra pour 14 habitants. Il n'en demeure pas moins que chaque jour nous nous retrouvons à de nombreuses reprises dans l'objectif de caméras dans les banques, les centres commerciaux, les garages de stationnement, les escaliers, les dépanneurs et, de plus en plus, dans des endroits publics comme les parcs et les rues.

Position du CPPP

Le Commissariat et la plupart des commissaires à la protection de la vie privée et des défenseurs du droit à la vie privée conviennent que la surveillance vidéo constitue une menace à la protection de la vie privée. Elle assujettit tous les gens à un examen minutieux par les forces de l'ordre ou d'autres autorités, qu'ils aient ou non posé un geste suspect. À tout le moins, elle circonscrit la « coquille » de la vie privée et de l'anonymat à laquelle nous avons droit lorsque nous vaquons à nos activités tout en respectant la loi, quand elle ne l'abolit tout simplement pas. Nous avons de bonnes raisons de croire que la surveillance vidéo a une incidence paralysante sur le comportement.

En 2001, le Commissariat a mené une enquête à la suite d'une plainte contre le recours à la surveillance vidéo par la GRC dans un parc public à Kelowna. L'enquête a conclu que la surveillance n'était pas justifiée, ce qui a donné lieu à de longues discussions avec la GRC qui insistait pour continuer d'utiliser le système bien qu'elle ait accepté de cesser l'enregistrement et de s'en servir uniquement à des fins de surveillance. La tentative de porter l'affaire devant les tribunaux s'est embourbée dans des questions de procédures et, en juillet 2003, le Commissariat a décidé de ne pas poursuivre l'enquête. Entre-temps, les services de police municipaux d'un nombre considérable de grandes villes canadiennes ont manifesté leur intérêt pour des systèmes publics de surveillance vidéo, certains d'entre eux ayant même décidé d'en installer.

vous utilisez votre carte de crédit pour payer un plein panier de marchandises dont chaque item peut être identifié par sa puce d'identification par radiofréquence, que le magasin que vous fréquentez utilise des caméras vidéo équipées d'une technologie de reconnaissance faciale. Maintenant, imaginez-vous qu'un ordinateur relie tous ces renseignements vous concernant à toutes les autres données provenant de votre carte de crédit, de la boîte noire, du GPS, des puces d'identification par radiofréquence et de toutes vos présences devant les caméras vidéo, puis les analyse afin de déceler les tendances de comportements à risque. Cet exemple est hypothétique mais il n'est certes pas inconcevable.

Position du CPVP

Ce défi a incité le Commissariat à mettre l'accent sur le renforcement de ses capacités de comprendre les nouvelles technologies et de composer avec elles. Il a par ailleurs lancé une série de conférences sur la vie privée auxquelles ont participé de nombreux invités éminents, lesquels ont présenté aux employés et aux membres de la collectivité des allocutions sur les enjeux du changement technologique et recommandé de nouvelles orientations. Il a, de plus, donné le coup d'envoi à un programme de contributions qui encourage les projets de recherche portant sur le point de convergence entre la vie privée et la technologie.

Nous sommes conscients, toutefois, que le problème ne relève pas de la technologie en soi, mais du défaut de bien en contrôler l'utilisation. Nous sommes fondamentalement d'avis que l'utilisation de ces technologies doit à tout le moins être gouvernée par les principes de pratiques équitables en matière de renseignements. Tel est le cas des technologies variées comme les cartes intelligentes, les enregistreurs de données (« boîtes noires ») et les puces d'identification par radiofréquence. Il faut dire aux gens quels renseignements sont recueillis à leur sujet, qui les recueille, et à quelles fins. Il faut leur dire quelle utilisation est faite de ces renseignements et à qui ils sont communiqués. Ils doivent pouvoir contrôler la collecte, l'utilisation et la communication des renseignements grâce à leur pouvoir d'accorder ou de refuser leur consentement. Les renseignements doivent être conservés en lieu sûr et considérés confidentiels. Les gens ont le droit d'avoir accès aux renseignements les concernant de même que le droit de les corriger au besoin.

Lorsque les technologies sont appliquées à la surveillance, elles sont assujetties à une norme encore plus rigoureuse. Leur mise en place et leur utilisation devraient être limitées aux circonstances particulières où elles sont justifiées, c'est-à-dire si elles répondent à un problème urgent et d'importance. Les allégations quant à leur caractère légitime doivent faire l'objet d'un examen minutieux et répondre à des critères sévères.

La technologie peut menacer la vie privée et ne cesse de préoccuper les défenseurs de la vie privée et les commissaires à la protection de la vie privée. Tel est surtout le cas lorsque des technologies d'observation de plus en plus perfectionnées et d'enregistrement des renseignements concernant le lieu où se trouvent des personnes, leurs déplacements, leur comportement et leurs gestes se greffent à des ordinateurs de plus en plus performants dans lesquels cette information est stockée, triée, appariée et analysée. Songez par exemple aux renseignements qui pourraient être recueillis à votre sujet lorsque vous rendez au magasin à bord de votre voiture munie d'un système mondial de localisation (GPS), que

Technologies de surveillance

carte nationale d'identité semble avoir été mise en veilleuse, il reste vigilant.

Le Commissariat maintient ce point de vue et, même si la proposition relative à une

bien trop élevé pour le droit à la vie privée.

À son avis, un système du genre présente des avantages minimes à un coût le défi de taille à relever pour le rendre pratique, abordable et respectueux de la vie privée. Son exposé a soulevé de nombreuses questions, notamment les risques et coûts appréciables associés à la mise sur pied d'un système national d'identification et devant le Comité permanent de la Chambre de la citoyenneté et de l'immigration. par intérêt, pour son analyse convaincante et réfléchie de l'enjeu qu'il a présentée a même félicité Robert Marleau, le Commissaire à la protection de la vie privée vue sur ces enjeux. Un éditorial paru le 22 septembre 2003 dans le *Globe and Mail* éditoriaux et chroniques dans les grands journaux qui se sont ralliés à nos points de Ses efforts ont abouti à une couverture médiatique positive ainsi qu'à de nombreux proposé à l'automne 2003.

Lors d'un débat sur cette question, le Commissariat s'est vivement opposé au projet de carte nationale d'identité que le ministre de la Citoyenneté et de l'Immigration a

Position du CPPP

d'identité leur caractère menaçant pour la vie privée.

à la piste et de surveiller cette personne. C'est bien ce pouvoir qui confère aux cartes d'appartenance des renseignements concernant une personne et, au bout du compte, de suivre secteur public et le secteur privé, peut représenter un moyen puissant de recueillir et Une carte unique, servant d'identificateur dans un vaste éventail d'opérations avec le accès à des renseignements personnels et permettant de les combiner et de les manipuler. d'une personne. Elle constitue également un outil de gestion de l'information donnant s'imbrique, ne représente pas simplement un outil pratique de confirmation de l'identité monde entier. Une carte d'identité, incluant le système d'identification dans lequel elle

Cartes d'identité

- cartes d'identité;
- technologies de surveillance et vidéo;
- accès du gouvernement aux fonds de renseignements personnels détenus par les entreprises;
- protection des renseignements personnels sur la santé;
- réglementation du droit à la vie privée dans un régime fédéral.

Au cours de la période visée par le rapport de 2003-2004, le Commissariat a réussi à promouvoir la protection du droit à la vie privée dans le cadre d'un éventail d'enjeux sociaux, technologiques et politiques, dont ceux qui sont énumérés ci-après :

Le droit à la vie privée des nouvelles lois et politiques.

Le Commissariat a déployé un effort concerté pour renforcer ses relations avec le Parlement et mieux répondre aux besoins de ce dernier. Dans cette optique, nous avons créé une nouvelle fonction d'agent de liaison parlementaire qui s'attachera précisément à informer les députés et sénateurs sur des questions particulières en matière de vie privée, à surveiller les initiatives législatives et réglementaires, de même qu'à prendre les mesures nécessaires pour que la Commissaire et les cadres supérieurs de notre organisation de l'effectif fournissent des conseils éclairés aux parlementaires au sujet des répercussions sur le droit à la vie privée ainsi que les moyens d'y réagir.

Une des principales attributions du Commissariat à la protection de la vie privée consiste à recenser et à analyser les nouveaux enjeux en matière de vie privée et d'élaborer des politiques et des positions qui les régleront et feront progresser le dossier de la protection du droit à la vie privée. La recherche et l'analyse que nous menons de ces enjeux stimulent et alimentent le débat public, suscitent l'engagement des Canadiens et des Canadiennes et accroissent la sensibilisation du public. Le Commissariat peut donc servir au Parlement de fenêtre sur les enjeux en matière de vie privée, fournir promptement des conseils éclairés sur l'incidence des initiatives législatives et réglementaires et faire connaître au grand public les risques qui menacent la protection de la vie privée ainsi que les moyens d'y réagir.

Depuis longtemps, les cartes d'identité sont source de préoccupation pour le Commissariat et pour les commissaires à la protection des données nominatives et de la vie privée du

En bout de ligne, les décisions que nous prenons maintenant en matière de vie privée et le fait que nous tenions réellement ou non à cette dernière façonneront la société que nous léguons à nos enfants. À titre d'organisme chargé de protéger le droit à la vie privée, nous devons confronter les personnes qui troqueraient volontiers les droits individuels contre la promesse d'une sécurité nationale ou de technologies portant atteinte à la vie privée. Nous devons veiller à ce que la grande valeur que les Canadiens et les Canadiennes accordent à leur droit à la vie privée ne soit pas perdue dans le tumulte des voix exigeant un accroissement de la sécurité et la collecte de renseignements supplémentaires sur tous autant que nous sommes. Nous devons à l'avenir concevoir nos efforts pour relever les défis qui nous attendent assurément.

Par ailleurs, nous avons constaté des progrès au chapitre des efforts législatifs déployés pour garantir le droit à la protection des renseignements personnels. Un représentant chargé de protéger les renseignements personnels versés aux dossiers publics a été nommé dans chaque province et chaque territoire. Trois provinces, l'Alberta, la Saskatchewan et le Manitoba, ont promulgué des lois portant précisément sur la protection des renseignements personnels sur la santé; l'Ontario vient tout juste d'adopter une loi semblable qui devrait entrer en vigueur plus tard en 2004. Le Québec, l'Alberta et la Colombie-Britannique ont édicté des lois régissant la collecte, l'utilisation et la communication de renseignements personnels dans le secteur privé.

à abandonner, réduire ou reporter nombre de mesures de lutte contre le terrorisme. Le programme *Operation TIPS*, qui devait assurer le concours de travailleurs comme des employés de sociétés de câblodistribution et de livraison de colis pour signaler des activités suspectes, a été abandonné. Le projet *Total Information Awareness*, qui aurait permis au gouvernement de recourir au « forage de banques de données » pour grouper et analyser des renseignements provenant de bases de données commerciales des secteurs public et privé n'a jamais pris son envol. Le programme *Computer Assisted Passenger Prescreening System* (CAPPS II), qui devait identifier les terroristes étrangers ou les personnes ayant des liens avec des terroristes, a lui aussi été abandonné en raison de préoccupations en matière de vie privée.

Au Canada, le public a fait connaître haut et fort son opposition à une carte nationale d'identité, si bien que la proposition a été mise en veilleuse. Le Commissariat à la protection de la vie privée du Canada a soulevé de graves objections à cette proposition et il continue de s'y opposer.

En septembre 2003, Robert Marleau, le Commissaire à la protection de la vie privée par intérim, a comparu devant le Comité permanent de la citoyenneté et de l'immigration pour discuter de l'opposition du Commissariat à la carte d'identité nationale. Denis Coderre, à l'époque ministre de la Citoyenneté et de l'Immigration, a prétendu qu'une telle carte constituerait une preuve d'identité plus sûre et plus fiable, qu'elle permettrait d'enrayer le vol d'identité, qu'elle faciliterait les déplacements des Canadiens et des Canadiennes à l'étranger et qu'elle empêcherait l'établissement de profils raciaux à la frontière.

Le Commissaire par intérim a exhorté le Comité à rejeter la proposition en invoquant les motifs suivants :

« Les risques associés à une carte d'identité nationale sont considérables. Les défis que pose la mise en œuvre d'un système national d'identification pratique, abordable et respectueux des droits à la vie privée des Canadiens et des Canadiennes sont colossaux. On n'a pas avancé d'arguments irréfutables en faveur d'un tel système; s'il y en avait, ceux-ci seraient, au mieux, marginaux. »

Plus de 60 témoins ont comparu devant le Comité et presque tous s'opposaient à l'instauration d'une carte nationale d'identité. Des groupes de protection du droit à la vie privée et des droits de la personne, des groupes de pression de consommateurs, des organisations religieuses et ethniques ainsi que des grands journaux de toutes les régions du Canada ont manifesté leur opposition à cette proposition.

La modification de la *LPRPD* est encore plus alarmante étant donné que ses retombées pourraient être encore plus vastes. En permettant aux organisations du secteur privé de recueillir des renseignements personnels sans le consentement de l'intéressé à la seule fin de les communiquer au gouvernement, aux forces de l'ordre et aux organismes de sécurité nationale, on les autorise en réalité à servir d'agents de l'État. Le fait d'autoriser une organisation à communiquer aux organismes gouvernementaux des renseignements qu'elle possède déjà sans le consentement de l'intéressé n'a absolument rien à voir avec le fait d'autoriser, voire d'encourager, une organisation du secteur privé à recueillir ces renseignements sans le consentement de l'intéressé, puis de les communiquer, une fois de plus, sans le consentement de l'intéressé. La modification vise toute organisation assujettie à la *LPRPD* et non seulement les transporteurs aériens. Elle ne limite aucunement la quantité de renseignements pouvant être recueillis sans le consentement de l'intéressé, pas plus qu'elle n'impose de limite aux sources de renseignements.

Ces dispositions estompent dangereusement la distinction entre le secteur privé et le secteur public, car elles assurent le concours des entreprises, non seulement pour lutter contre le terrorisme, mais aussi pour mener les activités conventionnelles d'application de la loi.

En dépit de notre opposition, de l'opposition de plusieurs de nos collègues provinciaux et territoriaux et de l'opposition d'un grand nombre d'autres organisations, le Sénat a adopté le projet de loi C-7, et la *Loi sur la sécurité publique* a reçu la sanction royale en mai 2004.

« Pour chaque action... »

Malgré tous les défis connus cette année, nous pouvons tout de même afficher un optimisme prudent. Si les menaces à l'encontre de la protection de notre vie privée ne cessent de croître, tel est également le cas de l'intérêt pour la défense du droit à la vie privée.

Nous entendons de plus en plus parler des puces d'identification par radiofréquence, des cellulaires-appareils photo, des enregistrateurs de données dans les voitures et des caméras de surveillance vidéo parce que le Commissariat à la protection de la vie privée, les groupes de protection des libertés civiles, les défenseurs de la vie privée et d'autres font connaître leurs préoccupations. De plus, les médias publient des reportages sur ces technologies parce qu'ils savent que le grand public s'intéresse à la protection de la vie privée.

L'opposition exprimée par des défenseurs de la vie privée, les médias et des politiciens de deux grands partis politiques des États-Unis a contraint l'administration américaine

l'information et à la protection de la vie privée de la Colombie-Britannique, a lancé un processus de consultations publiques pour examiner le dossier, dans le cadre duquel le Commissariat a déposé un document d'orientation sur la loi dite *USA PATRIOT Act*. Diverses mesures de lutte contre le terrorisme adoptées par les États-Unis supposent le recours aux bases de données du secteur privé pour confirmer l'identité ou déceler des tendances de comportements susceptibles d'indiquer qu'une personne constitue une menace. Nombre de ces initiatives, comme le programme *Terrorism Information Awareness*, font intervenir « le forage de banques de données », c'est-à-dire l'application de la technologie des bases de données et d'algorithmes complexes pour consulter des quantités massives de renseignements afin de détecter des tendances ou des corrélations cachées.

La Loi sur la sécurité publique

La distinction entre le secteur public et le secteur privé commence aussi à s'estomper au Canada, comme en fait surtout foi l'adoption récente du projet de loi C-7, la *Loi sur la sécurité publique*.

Il a fallu, pour que ce projet de loi très controversé devienne loi, deux ans et demi d'efforts et quatre tentatives.

En mars 2004, la Commissaire Stoddart a comparu devant le Comité sénatorial permanent sur les transports et les communications afin de commenter le projet de loi C-7. Ses commentaires ont porté sur deux volets du projet de loi, à savoir la modification de la *Loi sur l'aéronautique* qui autorise le Commissaire de la GRC et le directeur du Service canadien du renseignement de sécurité (SCRS) à demander aux transporteurs aériens et aux exploitants de systèmes de réservation de services aériens de leur fournir certains renseignements sur les passagers et la disposition modifiant la *Loi sur la protection des renseignements personnels et les documents électroniques (LPPDE)* afin de permettre aux organisations de recueillir des renseignements personnels sans le consentement de l'intéressé, lesquels renseignements seront communiqués au gouvernement, aux forces de l'ordre et aux organismes de sécurité nationale.

La GRC et le SCRS se serviront des renseignements sur les passagers pour identifier les personnes susceptibles de constituer une menace à la sécurité du transport et à la sécurité nationale, l'utilisation de ces renseignements constituant une fin légitime selon les dispositions de la *Loi sur la sécurité publique*. Toutefois, les renseignements peuvent également servir à exécuter des mandats d'arrestation pour la commission des infractions punissables d'une peine d'emprisonnement de cinq ans ou plus, fin qui n'a aucun lien avec la loi.

Le Commissariat à la protection de la vie privée est d'avis que nous ne devrions pas avoir à choisir le moindre de deux maux. Il faut trouver le juste milieu entre l'établissement de profils raciaux et la collecte d'une surabondance de renseignements sur tous et la surveillance accrue de tous. Le Commissariat n'est pas convaincu qu'en réduisant les libertés de tous les membres d'une société on réussisse à empêcher les terroristes de profiter d'autres menaces à la sécurité publique.

Le Commissariat ne s'oppose pas à l'amélioration de la sécurité. La question est toutefois de savoir comment nous pourrions y parvenir sans saper les valeurs fondamentales de notre société. Nous ne nous opposons pas à l'échange de renseignements entre les organismes, pourvu que des procédures et des politiques aient été instaurées pour les protéger, pour veiller à ce qu'ils soient utilisés ou communiqués uniquement aux fins précises déterminées — qui doivent être raisonnables — et qu'ils ne soient pas conservés plus longtemps que nécessaire.

L'utilisation plus efficace des renseignements dont nous disposons déjà et non la collecte de renseignements supplémentaires pourrait régler en partie le problème de l'accroissement de la sécurité. C'est bien le message que la vérificatrice générale a transmis dans son rapport de mars 2004. Le rapport cite plusieurs cas où des organismes et ministères canadiens ont omis de partager ou d'utiliser des renseignements en leur possession qui auraient accru la sécurité. Il précise notamment qu'en dépit du fait que plus de 25 000 passeports canadiens sont perdus ou volés chaque année, les fonctionnaires aux postes frontaliers ne reçoivent pas de listes de ces documents perdus ou volés.

La participation du secteur privé constitue une autre caractéristique troublante des mesures de sécurité nationale en voie d'être instaurées. La sécurité nationale, depuis toujours, a été confiée à des organismes gouvernementaux qui se fondaient essentiellement sur le renseignement de sécurité qu'ils recueillaient eux-mêmes. Or, les organismes de sécurité nationale se servent de plus en plus des renseignements personnels recueillis auprès des particuliers par le secteur privé à des fins non liées à la sécurité nationale. Ces données s'ajoutent aux renseignements déjà connus, et l'on s'en remet au savoir-faire du secteur privé pour élaborer les outils d'analyse nécessaires.

Cette situation soulève nombre de questions troublantes. En Colombie-Britannique, la proposition de confier l'administration des régimes provinciaux de soins de santé et d'assurance-médicaments à une filiale canadienne d'une entreprise américaine a suscité de nombreuses préoccupations. Les opposants craignent qu'ainsi, des organismes américains comme le *Federal Bureau of Investigation* n'obtiennent des renseignements personnels concernant les Canadiens et les Canadiennes auprès d'entreprises américaines conformément à la loi dite *USA PATRIOT Act*. David Loukidellis, le Commissaire à

Etats-Unis, à savoir l'initiative *Total Information Awareness* (qui est devenue *Terrorism Information Awareness*), le *Computer Assisted Passenger Prescreening System* (CAPPS II), lequel a été abandonné depuis en raison de préoccupations relatives à la vie privée, et le programme *VISIT*. Le système *Terrorism Information Awareness* vise l'intégration des bases de données commerciales et gouvernementales, ce qui donnera accès aux achats par carte de crédit, aux réservations de voyage, aux dossiers téléphoniques, aux dossiers de courriels, aux antécédents médicaux, à l'information financière et même à l'utilisation de la bibliothèque publique.

Cette importance accordée à la collecte de vastes quantités de renseignements personnels caractérise également les initiatives canadiennes. L'ASFC recueille actuellement des renseignements personnels sur tous les passagers du transport aérien qui arrivent au Canada dans le cadre de l'initiative *Information préalable sur les voyageurs* et du *dossier passager* (IPV/DP) dont il a été question dans les rapports annuels antérieurs. Ces renseignements sont utilisés aux fins du programme NEXUS et du programme EXPRES, lesquels permettent d'approuver au préalable la circulation entre les frontières canado-américaines des voyageurs et des envois commerciaux présentant peu de risques.

Plus de renseignements = plus de sécurité?

La plupart des textes de loi sur la lutte contre le terrorisme qui ont été adoptés au Canada et à l'étranger se fondent sur la prémisse que la sécurité de la population croît en fonction de l'augmentation du nombre de renseignements que le gouvernement recueille sur tous les particuliers, que leur comportement soit ou non suspect.

Nous apprenons que la collecte et l'utilisation de ces renseignements afin de déceler les menaces est le prix à payer pour éviter l'établissement de profils raciaux et ethniques et le recours aux stéréotypes. Nous recevons l'assurance que les outils d'évaluation des risques ne reconnaissent pas la couleur ni la religion, mais qu'ils se bornent à analyser l'information.

Les forces de l'ordre et les organismes de sécurité nationale recueillent de plus en plus de renseignements provenant de plus en plus de sources et concernant de plus en plus de personnes et s'en servent de plus en plus pour déceler d'éventuelles menaces. Il s'ensuit alors que les gens risquent davantage d'être l'objet d'une surveillance non justifiée, d'être indûment pris à parti et de ne pas recevoir un traitement équitable. Des erreurs ont déjà été commises et d'autres continueront d'être commises. Par ailleurs, le manque de transparence fait que nous pourrions ne jamais savoir pourquoi ces personnes ont été ciblées par erreur ni où le système a échoué.

Redéfinir la frontière

La frontière représente désormais beaucoup plus qu'une simple rivière ou une ligne tracée sur une carte et une série de postes de contrôle matériels. La frontière est en voie de devenir virtuelle, ce qui suscite des préoccupations en matière de vie privée. Comme le laisse supposer la création de l'ASFC, le programme de sécurité nationale du gouvernement du Canada est en grande partie axé sur la frontière. Il en découle un nouveau concept de ce que constitue une frontière. En décembre 2001, le Canada et les États-Unis ont signé la Déclaration sur la frontière intelligente. La *Politique de sécurité nationale* prévoit « créer une frontière du XXI^e siècle » et élaborer une « frontière intelligente de la prochaine génération avec le Mexique et les États-Unis ».

De plus en plus, les décisions concernant les personnes autorisées à entrer au Canada ou celles qui constituent une menace à la sécurité sont prises bien avant que les intéressés n'arrivent au Canada. Dans bon nombre de villes, les voyageurs qui prennent l'avion en direction des États-Unis peuvent passer aux douanes américaines par un aéroport canadien. En ce qui concerne les cybermenaces, la notion conventionnelle de frontière n'a plus aucune importance : les cyberattaques peuvent provenir de n'importe où dans le monde. C'est pourquoi la nouvelle *Politique de sécurité nationale* prévoit que « le gouvernement créera aussi un groupe de travail national de haut niveau, composé de représentants des secteurs public et privé, en vue d'élaborer une stratégie nationale de cybersécurité. Cette stratégie réduira la vulnérabilité du Canada aux cyberattaques et aux cyberaccidents. »

La frontière nationale perd de son importance. La politique de sécurité frontalière des États-Unis est fondée sur la création d'une zone tampon ou d'un cordon sanitaire entourant l'Amérique du Nord et, de plus en plus, les politiques canadiennes abondent dans ce sens. Notre sécurité frontalière commence à s'intégrer avec celle des États-Unis. Le Canada et les États-Unis ont mis sur pied plusieurs équipes intégrées de la police multidisciplinaire des frontières. Les deux pays échangent des listes de surveillance, et on presse le gouvernement du Canada de procurer au gouvernement des États-Unis des renseignements concernant toute personne provenant d'un pays étranger qui se rendrait au Canada.

La frontière intelligente ou la frontière virtuelle suppose la collecte de renseignements personnels, de vastes quantités de renseignements personnels. Cette information sert à vérifier l'identité et à déterminer qui devrait pouvoir entrer au pays sans subir d'examen, qui devrait faire l'objet d'une surveillance et qui devrait s'en voir refuser l'admission. C'est surtout ce qui ressort des diverses initiatives mises en œuvre ou proposées par les

prépare des lignes directrices sur l'utilisation de la surveillance vidéo par les forces de l'ordre et les particuliers peuvent se renseigner sur les logiciels espions afin de se protéger.

Accroître la sécurité : à quel prix?

En bout de ligne, les mesures accrues de sécurité que déploient les gouvernements du monde entier peuvent constituer une menace plus fondamentale et troublante à nos droits fondamentaux, ce qui comprend notre droit à la vie privée. Les récentes tentatives visant à augmenter notre sécurité et notre protection, à la fois contre le terrorisme international et contre les menaces plus conventionnelles à la sécurité publique, soulèvent de très graves préoccupations en matière de vie privée.

Partout dans le monde, des gouvernements, dont celui du Canada, continuent d'installer des mesures accrues de sécurité en supposant que, si les forces de l'ordre et les organismes de sécurité nationale disposent de suffisamment de renseignements personnels nous concernant tous, notre société sera plus sûre et plus protégée. En décembre 2003, le gouvernement du Canada a créé l'Agence des services frontaliers du Canada (ASFC), regroupant ainsi les fonctions de sécurité frontalière et du renseignement de l'Agence des douanes et du revenu du Canada, de Citoyenneté et Immigration Canada et de l'Agence canadienne d'inspection des aliments. Quant à elle, l'ASFC fait partie du nouveau ministère de la Sécurité publique et de la Protection civile aux côtés du Service canadien du renseignement de sécurité (SCRS) et de la Gendarmerie royale du Canada (GRC).

En avril 2004, le gouvernement du Canada a publié sa tout première *Politique de sécurité nationale* qui propose notamment de créer un « centre d'évaluation intégrée des menaces » qui facilitera la collecte et l'analyse du renseignement et d'autres informations. Le document sur la politique gouvernementale prétend que le centre « aidera à réduire les risques que l'information que possède un secteur de la fonction publique ne soit pas communiquée promptement à ceux auxquels cette information peut être utile ».

Le gouvernement du Canada a fait savoir qu'en 2005, il commencera à délivrer des passeports dotés d'une technologie biométrique de reconnaissance faciale. Cette proposition n'a jamais été une proposition officielle du gouvernement, mais au moins un ministre du Cabinet a préconisé l'installation d'une carte nationale d'identité.

s'installe subrepticement sur votre ordinateur, puis transmet en secret de l'information sur vos activités en ligne à votre insu et sans votre consentement. Le logiciel espion est souvent greffé à un courriel non sollicité, de sorte que vous pourriez ne pas savoir comment les programmes ont été installés sur votre appareil ni même comment les enlever.

Protéger votre droit à la vie privée

Ces technologies ont attiré passablement notre attention au cours de la dernière année, mais, dans la plupart des cas, les menaces qu'elles posent peuvent être examinées grâce à l'application de principes de pratiques équitables en matière de renseignements. Ces principes sont énoncés dans la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* qui régit la collecte, l'utilisation et la communication des renseignements personnels vous concernant.

Les formulations de ces principes sont nombreuses, mais elles peuvent se résumer ainsi :

- la collecte, l'utilisation et la communication des renseignements personnels ne peuvent se faire à l'insu de l'intéressé et sans son consentement;
- les organisations ne doivent recueillir que les renseignements dont elles ont besoin;
- les organisations doivent expliquer pourquoi elles recueillent les renseignements et ces derniers ne doivent être utilisés que pour les fins déterminées;
- les intéressés devraient pouvoir corriger ou modifier les renseignements les concernant;
- les organisations doivent instaurer des politiques et pratiques régissant la collecte, l'utilisation et la communication de renseignements personnels, ce qui comprend des politiques de destruction et des procédures de sauvegarde des renseignements.

Ces technologies de surveillance présentent sans aucun doute de grandes menaces d'intrusion dans notre vie privée et de compromission de la protection de nos renseignements personnels, mais il existe des moyens d'en atténuer l'incidence. Une coalition d'organismes de protection de la vie privée des consommateurs et de défense des droits civils a publié un exposé de principe sur l'utilisation responsable des puces d'identification par radiofréquence. Le Commissariat

Le logiciel espion, une nouvelle technologie de surveillance, a remplacé les « témoins » à titre de menace la plus récente à la vie privée sur Internet. Il s'agit d'un logiciel qui

Si vous portez un vêtement contenant une de ces puces, le détaillant pourrait vous identifier dès votre entrée dans le magasin. Le gouvernement pourrait un jour suivre à la piste les déplacements des visiteurs qui sont entrés au pays.

Au cours de la dernière année, nous avons pris connaissance de l'expression « puces d'identification par radiofréquence ». Il s'agit de circuits informatiques miniatures munis de toutes petites antennes qui signalent leur présence en vibrant et qui sont dotés d'un code d'identification unique. Sans être nouvelles, ces puces suscitent actuellement une certaine inquiétude. Elles servent déjà à de nombreuses fins; on les retrouve notamment dans les *porte-clés* émis par les postes d'essence grâce auxquels les clients peuvent payer leurs achats aux pompes. À l'heure actuelle, les détaillants et les gouvernements proposent d'insérer ces puces dans presque tout, depuis les documents de voyage jusqu'au papier-monnaie et même certains vêtements. C'est la capacité de lecture à distance de ces puces qui soulève

Tous les jours, nous lisons dans les médias des articles sur les nouvelles technologies ou les nouvelles utilisations de technologies existantes qui menacent notre vie privée. Des systèmes mondiaux de localisation qui repèrent par satellites l'emplacement des véhicules et suivent leurs déplacements sont installés dans des automobiles de location et les véhicules des employés. Les cellulaires-appareils photo pouvant capter et transmettre subrepticement des images sont utilisés pour porter atteinte à la vie privée des gens. De plus en plus de municipalités envisagent l'installation de caméras de surveillance vidéo au centre-ville.

Technologies de surveillance subreptice

De presque tous les points de vue, l'année écoulée s'est révélée des plus difficiles pour la protection de la vie privée. En raison de la prolifération des menaces, la lutte pour protéger le droit à la vie privée des Canadiens et des Canadiennes et pour protéger les renseignements personnels a exigé à maintes reprises des efforts sans relâche. Les perspectives ne sont toutefois pas tout à fait sombres.

crises. J'affirme avec fierté que le Commissariat a profité de l'opportunité qui lui a été offerte pour renforcer ses assises et, fort de son énergie renouvelée, il pourra relever avec confiance les nombreux défis en matière de protection du droit à la vie privée qui s'annoncent.

De nouvelles technologies voient le jour et menacent la vie privée de manières encore jamais vues. Nous continuerons de surveiller l'utilisation et l'incidence de technologies telles que la surveillance vidéo, les logiciels espions, les dispositifs d'identification par radiofréquence, les systèmes mondiaux de localisation, les dispositifs de communication sans fil ainsi que les identificateurs biométriques comme la reconnaissance faciale, l'ADN et les empreintes digitales. Le Commissariat concerte ses efforts à ceux de ses partenaires fédéraux afin de trouver les mesures juridiques, réglementaires et techniques qui permettront de traiter de ces enjeux.

À titre d'exemple, nous avons été témoins de la prolifération des pourriels, ces courriels non sollicités très répandus, qui commencent à menacer sérieusement la vie privée et l'intégrité des renseignements personnels concernant les Canadiens et les Canadiennes. Les pourriels sont souvent porteurs de codes informatiques malveillants qui infectent votre ordinateur et créent des programmes capables de lire vos courriels, de suivre l'utilisation que vous faites d'Internet et même de dérober vos mots de passe et numéros de cartes de crédit. Le Commissariat travaille de près avec Industrie Canada et son groupe de travail anti-pourriel afin de trouver des moyens de juguler cet épineux problème et d'aider les consommateurs à prendre des mesures concrètes et efficaces pour se protéger. De même, nous nous pencherons sur les possibilités de sauvegarder le droit à la vie privée des consommateurs en analysant l'incidence négative éventuelle des nouvelles technologies qui soulèvent des préoccupations en matière de vie privée.

Au cours de la prochaine année, le Commissariat poursuivra ses efforts de communication pour sensibiliser la population canadienne et les entreprises canadiennes afin que celles-ci comprennent mieux leurs droits et obligations aux termes de la *Loi sur la protection des renseignements personnels* et de la *LPRPDE*. Nous tenterons par divers moyens d'obtenir le point de vue des Canadiens et des Canadiennes afin de mieux combler leurs besoins et pour renforcer le rôle du Commissariat à la protection de la vie privée à titre d'autorité assurant la protection et la promotion du droit à la vie privée.

Surtout, je tiens à profiter de l'occasion du dépôt de mon premier rapport à titre de Commissaire à la protection de la vie privée pour faire l'éloge des employés du Commissariat, qui ont su surmonter des difficultés sans précédent, sur le plan personnel tout autant qu'administratif, afin de s'acquitter de leurs responsabilités. Leur professionnalisme, leur engagement à maintenir le droit à la vie privée de la population canadienne, leur respect des principes de la fonction publique et leur courage devant l'adversité méritent certes d'être soulignés. L'année a été semée d'embûches, mais les opportunités naissent souvent des

Même si le Commissariat a traversé une période marquée par les difficultés, il a poursuivi ses travaux de surveillance des tendances et initiatives technologiques afin d'aider à protéger le droit à la vie privée de la population canadienne et à assurer l'intégrité des renseignements personnels et ce, en présence des nouvelles menaces à la vie privée qui se font sentir à l'échelle tant nationale qu'internationale. Au début de l'année, l'idée d'une carte d'identité nationale a été lancée, à laquelle nombre de Canadiens et de Canadiennes se sont opposés. Cette idée a été mise en veilleuse, du moins jusqu'à maintenant. La plupart des Canadiens et des Canadiennes ayant comparu devant le Comité permanent sur la citoyenneté et l'immigration, y compris des représentants du Commissariat, ont manifesté leur vive opposition à l'instauration d'une telle carte d'identité. Nous continuons de nous y opposer.

La collecte, l'enregistrement, le tri et le partage d'une quantité alarmante de renseignements personnels concernant les Canadiens et les Canadiennes se sont poursuivis en conformité du principe, non démontré cependant, selon lequel l'augmentation du nombre de renseignements concernant les particuliers se traduit par une plus grande protection contre le terrorisme et les autres menaces. Nous nous inquiétons de l'intégration croissante de notre sécurité frontalière à celle des États-Unis, laquelle donne lieu à une collecte de vastes fichiers de renseignements personnels sur les voyageurs, les éventuels voyageurs et les employés de l'industrie du transport qui sont appelés à traverser régulièrement la frontière dans l'exercice de leurs fonctions. Le Commissariat examine de très près les pratiques de traitement des renseignements personnels de l'Agence des services frontaliers du Canada qui vient d'être mise sur pied.

Le dossier de la circulation transfrontalière des données a également suscité notre attention cette année. Dans un monde de plus en plus informatisé, il suffit de cliquer sur une souris pour envoyer dans toutes les régions du globe des renseignements personnels concernant les Canadiens et les Canadiennes. Nous nous inquiétons de l'incidence que cela peut avoir sur le droit à la protection de la vie privée de la population canadienne. Le Commissariat mène un projet qui permettra d'identifier les circuits d'acheminement des renseignements personnels entre les frontières et de déterminer les droits et mesures de protection susceptibles de s'appliquer à ces renseignements. Nous sommes conscients de la nécessité d'accroître la sécurité de l'environnement public actuel et nous ne nous opposerons jamais aux mesures légitimes de lutte contre le terrorisme. Toutefois, il faut arriver à assurer un équilibre entre, d'une part, la sécurité nationale et internationale et, d'autre part, le droit fondamental à la vie privée des personnes et le droit de la personne de contrôler la collecte, l'utilisation et la communication des renseignements personnels à son sujet.

Colombie-Britannique. Le Commissariat collabore avec ses homologues provinciaux afin de trouver une démarche harmonisée de règlement des plaintes en matière de vie privée et poursuivra ses efforts en ce sens.

Ainsi, la *LPRPD* touche les organisations, des grandes entreprises aux petits dépanneurs, des multinationales de l'industrie de la finance et de l'assurance aux fleuristes et aux nettoyeurs de quartier. Au départ, les nouvelles règles régissant les renseignements personnels dans le secteur privé ont été source de confusion et d'inquiétude.

Toutefois, au cours de l'année et, surtout dans les mois qui ont précédé la date butoir du 1^{er} janvier 2004, nous avons cherché activement à aider les organisations à mettre en œuvre la *LPRPD* et à s'y conformer. Nous nous sommes engagés dans la voie de la sensibilisation, de la coopération, de l'éducation du public ainsi que de la conclusion de nouveaux partenariats novateurs avec le secteur privé. Nous avons mené de vastes consultations auprès des associations commerciales du secteur privé, en particulier avec celles du secteur bancaire et financier et avec l'industrie du marketing direct. Pendant l'année écoulée, la Commissaire adjointe à la protection de la vie privée, Heather Black, a sillonné le pays et prononcé un très grand nombre d'allocutions devant des groupes des plus variés afin de sensibiliser davantage la population à la *LPRPD*. Avant sa nomination à titre de Commissaire adjointe, M^{re} Black a été avocate générale au Commissariat et à l'Industrie Canada, où elle a collaboré à la rédaction de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Nous avons de plus donné suite à des milliers de requêtes et de demandes de renseignements sur la *LPRPD* que nous ont adressées des entreprises et des organisations de toutes les régions du Canada. Nous avons consulté des groupes et associations commerciaux et envoyé des milliers de copies de rapports, de guides à l'intention des entreprises, de feuilles d'information et d'autres documents de sensibilisation du public. De plus, nous avons réorganisé et revampé notre site Web de sorte qu'il soit conforme à la normalisation des sites Internet et nous avons offert sur support électronique plusieurs ressources, guides et outils de conformité nouveaux à l'intention des entreprises et des particuliers au Canada.

L'année s'est également révélée exceptionnelle en ce qui concerne les plaintes déposées conformément à la *Loi sur la protection des renseignements personnels*. Le Commissariat a reçu un nombre record de nouvelles plaintes, qui ont enregistré une hausse de 250 pour 100 par rapport à l'année précédente. Le présent rapport contient un supplément de précisions qui expliquent ces statistiques. En outre, les enquêteurs ont traité un nombre inégalé de plaintes, réalisation fort louable compte tenu des défis supplémentaires que les employés ont dû relever au cours de l'année.

l'engagement des employés et des représentants syndicaux dans la reconstruction et le maintien d'un processus d'apprentissage organisationnel.

La création d'un plan de recouvrement des coûts et la mise au point d'un procédé complet de planification visant à réaligner nos stratégies et nos buts sont au nombre des autres mesures couronnées de succès. Un rapport préliminaire au Parlement sur les mesures prises à la suite du *Rapport sur le Commissariat à la protection de la vie privée du Canada* de la vérificatrice générale, déposé conjointement par le Commissariat et la présidente du Conseil du Trésor du Canada le 31 octobre 2003, a fourni en détail la liste des actions qui ont été prises ou qui seront prises quant aux mesures de recouvrement du Commissariat. La version finale du rapport a été déposée en avril 2004.

Nous avons en outre mis sur pied un comité consultatif externe, composé d'éminents experts nationaux de la protection de la vie privée, à qui nous avons demandé de prodiguer des conseils et des directives au Commissariat quant à ses orientations et priorités stratégiques. Par ailleurs, nous avons créé un comité consultatif patronal-syndical, de même qu'un comité de santé et sécurité afin de rétablir le bien-être global du milieu de travail. Nous nous activons également, de concert avec le Secrétariat du Conseil du Trésor, à améliorer notre service des ressources humaines. Par nos efforts de renouveau, nous avons essentiellement tenté de regagner la confiance du Parlement du Canada et, dans cette optique, nous avons créé un nouveau poste, celui d'agent de liaison parlementaire, grâce auquel nous pourrions nous acquitter de nos responsabilités permanentes à titre de fenêtre unique du Parlement sur les enjeux du droit à la vie privée.

Tout au long de cette année marquée par les difficultés et les bouleversements, le Commissariat s'est préparé à mettre en œuvre intégralement la *Loi sur la protection des renseignements personnels et les documents électroniques*, connue également sous l'acronyme *LPRPDE*. Depuis le 1^{er} janvier 2004, la *LPRPDE*, dont l'application s'est faite progressivement, régit la collecte, l'utilisation et la communication de renseignements personnels dans le cadre d'activités commerciales dans toutes les provinces autres que celles ayant promulgué une loi sur la protection des renseignements personnels que le gouvernement fédéral aura jugée « essentiellement similaire » à la loi fédérale.

La *LPRPDE* constitue une loi souple et pragmatique qui traite des enjeux relevant de plusieurs secteurs de compétence qui surviennent dans notre cadre constitutionnel. La *Loi* peut être remplacée par des textes de loi jugés « essentiellement similaires » à la loi fédérale. À la publication du présent rapport, seule la loi du Québec a été jugée essentiellement similaire, mais nous nous attendons à des constatations positives quant aux lois sur la protection des renseignements personnels adoptées par l'Alberta et la

L'année écoulée s'est révélée exceptionnelle pour le Commissariat à la protection de la vie privée du Canada. Le 1^{er} décembre 2003, lorsque j'ai été nommée au poste de commissaire, j'ai pris les rênes d'un bureau qui venait de subir de grands bouleversements. En l'espace de six mois, un commissaire et plusieurs hauts fonctionnaires ont remis leur démission à la suite de scandales et d'une attention médiatique soutenue, un commissaire intérimaire a été nommé, de nombreux examens, vérifications et enquêtes internes et externes ont été menés (dont certains se poursuivent toujours), deux commissaires

adjoints ont été nommés et l'organisation a été restructurée en profondeur. J'ai donc pris la barre d'un navire qui, malgré l'orientation positive que lui avait donnée le Commissaire à la protection de la vie privée par intérim, Robert Marleau, naviguait toujours dans les eaux troubles des crises administratives, financières et organisationnelles.

D'immenses progrès ont été réalisés au chapitre du renouveau institutionnel et du renforcement du cadre financier et de gestion du CPVP. Ces progrès ont contribué au tout premier plan à restructurer le Commissariat et à mieux faire valoir les efforts déployés pour accroître l'efficacité de notre organisme et faire en sorte qu'elle respecte les principes de la fonction publique tout en remplissant son mandat de protéger et de défendre le droit fondamental à la vie privée des Canadiens et des Canadiennes.

Je tiens à signaler le travail formidable que le commissaire par intérim Robert Marleau a abattu pour assurer le progrès du Commissariat en cette période difficile et complexe. Le soutien de M. Marleau et l'encouragement qu'il a su donner au personnel, sa collaboration avec les équipes de vérification et d'enquête ainsi que l'importance qu'il a accordée à la responsabilité et au travail d'équipe ont jeté de solides assises qui garantiront le retour à la normale. Il mérite notre appréciation et notre gratitude.

Pour construire sur ces assises, nous avons pris et nous continuons de prendre des mesures correctives afin de rétablir le bien-être global du milieu de travail, de renforcer davantage les pratiques de gestion et les contrôles financiers, de donner plus de transparence et d'équité au service des ressources humaines, de favoriser l'innovation et d'obtenir



TABLE DES MATIÈRES

Préface.....	1
APERÇU.....	7
Point de vue de la politique.....	17
Lois provinciales essentiellement similaires.....	27
Première partie — Rapport concernant la Loi sur la protection des renseignements personnels.....	31
Introduction.....	31
Enquêtes et demandes de renseignements.....	32
Plaintes en vertu de la Loi sur la protection des renseignements personnels.....	33
Définitions des conclusions aux termes de la Loi sur la protection des renseignements personnels.....	33
Cas choisis en vertu de la Loi sur la protection des renseignements personnels.....	33
Incidents visés par la Loi sur la protection des renseignements personnels.....	34
Incidents visés par la Loi sur la protection des renseignements personnels.....	42
Communication dans l'intérêt du public aux termes de la Loi sur la protection des renseignements.....	44
Examens et pratiques en matière de vie privée.....	54
Évaluations des facteurs relatifs à la vie privée.....	61
Devant les tribunaux.....	63
Deuxième partie — Rapport concernant la Loi sur la protection des renseignements personnels et les documents électroniques.....	65
Introduction.....	65
Enquêtes et demandes de renseignements.....	66
Définitions des conclusions en vertu de la LPRPD.....	66
Cas choisis en vertu de la LPRPD.....	67
Incidents visés par la LPRPD.....	91
Examens et pratiques en matière de vie privée.....	94
Devant les tribunaux.....	95
Troisième partie — Gestion intégrée.....	107



Novembre 2004

L'honorable Peter Milliken, Député
Président
Chambre des communes
Ottawa

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1^{er} avril 2003 au 31 mars 2004 conformément à la Loi sur la protection des renseignements personnels et celle du 2 janvier au 31 décembre 2003 conformément à la Loi sur la protection des renseignements personnels et les documents électroniques.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

La Commissaire à la protection
de la vie privée du Canada

Jennifer Stoddart

Jennifer Stoddart



Novembre 2004

L'honorable Daniel Hays, Sénateur
Président
Sénat du Canada
Ottawa
Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1^{er} avril 2003 au 31 mars 2004 conformément à la *Loi sur la protection des renseignements personnels* et celle du 2 janvier au 31 décembre 2003 conformément à la *Loi sur la protection des renseignements personnels* et les documents électroniques.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

La Commissaire à la protection
de la vie privée du Canada

Jennifer Stoddart

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-8210, 1-800-282-1376
Télec. : (613) 947-6850
TDD (613) 992-9190

© Ministre des Travaux publics et Services gouvernementaux Canada 2004
No de cat. IP50-2004
ISBN 0662-68421-4

Cette publication est également disponible sur notre site Web à www.privcom.gc.ca



Rapport annuel au Parlement
2003-2004

Privacy Commissioner
of Canada



Commissaire à la protection
de la vie privée du Canada



Rapport annuel au Parlement
2003-2004

Vie Privée

Commissaire à la protection
de la vie privée du Canada



Privacy Commissioner
of Canada



